FACULTAD DE POSTGRADO

TRABAJO FINAL DE GRADUACIÓN

BRECHA DE CONOCIMIENTO EN LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA ADMINISTRATIVA EN EL SECTOR FARMACÉUTICO HONDUREÑO: ESTUDIO DE CASO EN DISTRIBUIDORA LETERAGO Y LABORATORIO MEGALABS 2025

SUSTENTADO POR:

CHRISTIAN ANTONIO YANES HERRERA

FIDEL ERNESTO GARCÍA GUTIÉRREZ

PREVIA INVESTIDURA AL TÍTULO DE

MÁSTER EN

GESTIÓN DE TECNOLOGÍAS DE LA INVESTIGACIÓN

TEGUCIGALPA, M.D.C, HONDURAS, C.A.

FEBRERO, 2026

UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA

UNITEC

FACULTAD DE POSTGRADO

AUTORIDADES UNIVERSITARIAS

RECTORA

ROSALPINA RODRÍGUEZ

VICERRECTOR ACADÉMICO NACIONAL

JAVIER ABRAHAM SALGADO LEZAMA

SECRETARIO GENERAL

ROGER MARTÍNEZ MIRALDA

DECANA FACULTAD DE POSTGRADO

ANA DEL CARMEN RETTALLY VARGAS

BRECHA DE CONOCIMIENTO EN LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA ADMINISTRATIVA EN EL SECTOR FARMACÉUTICO HONDUREÑO: ESTUDIO DE CASO EN DISTRIBUIDORA LETERAGO Y LABORATORIO MEGALABS 2025

TRABAJO PRESENTADO EN CUMPLIMIENTO DE LOS REQUISITOS EXIGIDOS PARA OPTAR AL TÍTULO DE

MÁSTER EN
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

ASESOR
JESUS RICARDO RODRÍGUEZ RIVERA

MIEMBROS DE LA TERNA:
ALBA GABRIELA GARAY ROMERO
CARLOS AMADOR
JUAN CARLOS ALMENDAREZ

GRADUATE SCHOOL

KNOWLEDGE GAP IN INFORMATION SECURITY RISK MANAGEMENT FOR THE ADMINISTRATIVE AREA IN THE HONDURAN PHARMACEUTICAL SECTOR: CASE STUDY AT DISTRIBUIDORA LETERAGO AND LABORATORIO MEGALABS 2025

Christian Antonio Yanes Herrera

Fidel Ernesto García Gutiérrez

Abstract

This research examines the knowledge gap in Information Security (InfoSec) risk management at the Honduran subsidiary of Distribuidora Leterago (Megalabs group), a major player with a significant presence in the Latin American pharmaceutical sector. Our aim is to estimate the impact of this gap and its relationship to exposure to vulnerabilities and operational efficiency. The study is based on a situational diagnosis that reveals structural and regulatory gaps, as well as the absence of a formal and standardized risk management model aligned with international frameworks, which limits the identification, assessment, and systematic treatment of information risks and results in prolonged response times and greater exposure to threats such as phishing.

Consequently, an applied research project is proposed, based on an exploratory design and a particular case study, combining triangulation strategies: a competency matrix based on ISO 27005 to measure the knowledge of IT staff; surveys of leaders and administrative staff; and documentary analysis of policies and incidents. The analysis plan incorporates operational indicators, such as the Mean Time to Respond (MTTR), for incidents over the last twelve months, to link the knowledge gap with performance results.

The theoretical framework contextualizes the case through a macro (PESTEL) and micro analysis of the environment and substantiates the need for governance and continuous improvement in information security.

With this approach, the research seeks to quantify the skills and practices gap compared to ISO 27005; analyze cultural and policy factors that perpetuate it; and generate a baseline diagnosis to guide mitigation strategies during the fourth quarter of 2025.

The expected contribution includes implementation and prioritization guidelines that articulate competencies, processes, and technology with reference standards, reinforcing IT governance and operational resilience in the Honduran pharmaceutical context.

Keywords: Information Security risk management; InfoSec; ISO 27005; MTTR; pharmaceutical industry; Honduras.

DEDICATORIA

- Christian

Dedico todo el esfuerzo puesto en este proceso a todos los mencionados en la sección de agradecimiento, pero, hago especial énfasis en dedicar este material a todos aquellos que persiguen sus sueños y metas profesionales con fervor, especialmente a aquellos que trabajan y estudian a la vez, ahora puedo constatar que es tremendamente difícil lograrlo, a aquellos que además de trabajar y estudiar son el sustento económico de sus familias, honestamente, mis respetos.

- Fidel

Quisiera dedicar el esfuerzo que realicé durante todo este proceso académico a las personas que han creído en mi cuando ni siquiera yo mismo lo hice, por hacerme ver que el mundo está lleno de retos y es nuestro propósito como seres humanos encontrar aquellos que nos hagan sentir satisfechos con nuestras vidas; a aquellas personas que cada día desean salir adelante y superarse en un mundo lleno de adversidades, mi esfuerzo va para ustedes porque quiero hacerle saber a todos y todas que un mundo mejor es posible si todos ponemos de nuestra parte.

AGRADECIMIENTO

- Christian

Ha sido un largo recorrido para llegar a la culminación de nuestra tesis, agradezco a Dios la oportunidad de permitirme llegar hasta este punto, a mi familia por su apoyo incondicional en todo momento y aspecto, a mi compañero de lucha en este proceso, Fidel García, sin su apoyo gran parte de esta obra no habría sido posible y agradezco que no me haya dejado "tirar la toalla". A mis amistades por comprender cuando no podía asistir a un evento por darle prioridad a la maestría. A mi jefe por su gestión para obtener la aprobación de uso de datos de la empresa, Distribuidora Leterago. A mi mascota "Bonita" por esos momentos de risa y relajación brindados cuando mis ánimos están por los suelos, y por desvelarse conmigo incontables veces. Y sin ánimos de ser egocéntrico, a mí mismo por todo el esfuerzo puesto en estos dos últimos años. Gracias.

- Fidel

Es increíble darse cuenta de que el tiempo es efímero y cada día tenemos que hacer que nuestro suspiro en este mundo terrenal valga la pena, parte de esto es saber a quién agradecer por los logros que no serían posibles sin las personas que nos rodean. Quiero agradecerle a mi pareja Arantxa, a mis papás y a mis mejores amigos por darme fuerzas para seguir intentando lo mejor que pueda y expandir mis conocimientos para poder aplicarlos en proyectos o trabajos que aporten bien al mundo. Agradecerle a mi compañero Christian por su apoyo incondicional en todo este proceso donde nos desvelamos, pataleamos pero sobre todo, salimos victoriosos y eso es lo mejor que pudo haber pasado. A Distribuidora Leterago por permitirnos utilizar sus datos para crear conocimientos que pueden ser de gran ayuda, y por último, a mí mismo, que siempre tengo el deseo de salir adelante y ser una mejor versión que ayer. Gracias a todos y todas.

ÍNDICE DE CONTENIDO

CAPÍTULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1 INTRODUCCIÓN

La gestión de riesgos en las Tecnologías de la Información se ha consolidado como un componente crítico para la sostenibilidad de las empresas, la resiliencia organizacional y la continuidad del negocio, especialmente en sectores altamente regulados como el farmacéutico. Sin embargo, dentro de este contexto, se deberá comprender la forma en que la brecha de conocimiento, en materia de gestión de riesgos de la seguridad de la información específicamente, afecta la identificación, el tratamiento y el seguimiento de amenazas que resulta esencial para evaluar la exposición a vulnerabilidades y su impacto en la eficiencia operativa de las organizaciones.

El presente análisis se enmarca en la Distribuidora Leterago y Laboratorio Megalabs, siendo más específico, sus filiales hondureñas, considerada una importante compañía en el área de distribución y gestión de productos farmacéuticos en Latinoamérica. El propósito es diagnosticar eficazmente la brecha de conocimiento en gestión de riesgos de seguridad de la información existente y dar respuesta con fundamentos sólidos a los objetivos y preguntas planteadas inicialmente desde el capítulo I y que sea la base para generar futuras estrategias de mitigación de riegos para el área de TI de la mano de normas internacionales como la ISO 27005.

La estructura de esta tesis corresponde a una estructura de investigación vertical, donde cada capítulo se articula con el problema de investigación, las preguntas, los objetivos y la metodología seleccionada. De esta manera, se garantiza que los componentes teóricos, metodológicos y analíticos dan pie hacia la obtención de conclusiones orientadas a la toma de decisiones.

En el capítulo I expone el planteamiento de la investigación mediante una contextualización del problema, sus antecedentes y la formulación de la problemática central. Asimismo, se presentan las preguntas generales y específicas de investigación, los objetivos correspondientes y la justificación teórica del estudio.

El capítulo II desarrolla el marco teórico que sustenta la investigación. En él se examina el macroentorno regulatorio, tecnológico y económico de países comparables, así como el microentorno regional vinculado al mercado farmacéutico centroamericano. Establece el marco

conceptual y la relevancia que motiva la exploración de la brecha de conocimiento en la gestión de riesgos de TI en la Distribuidora Leterago y se analizan los principales marcos, metodologías y estándares relacionados con la gestión de riesgos de seguridad de la información, entre ellos ISO 27005 y NIST. Adicionalmente, se presenta un análisis crítico de las metodologías analizadas, las herramientas utilizadas y el marco legal que enmarca el trabajo, garantizando así una base sólida y multidimensional para el desarrollo de la investigación.

El capítulo III describe la metodología empleada, la cual se sustenta bajo un diseño de enfoque tipo mixto y en una estrategia de triangulación que integra datos cualitativos y cuantitativos. Se detalla la matriz de coherencia metodológica, la operacionalización de variables, y muy importante, el conjunto de hipótesis a ser probadas con el desarrollo de esta investigación, los criterios de muestreo, los instrumentos de recolección de información, en nuestro caso, encuestas, matriz de competencias, análisis documental y el plan analítico, que incorpora métricas como el Tiempo Medio de Respuesta (MTTR) de incidentes.

El capítulo IV presenta los resultados del análisis exploratorio de datos, el informe del proceso de recolección y los hallazgos encontrados a partir de la aplicación de los instrumentos seleccionados. Se examinan los resultados cuantitativos y cualitativos, se interpretan patrones, se vinculan los hallazgos con los objetivos y preguntas planteadas y se realiza un análisis estadístico y temático apoyado en la triangulación metodológica. Este capítulo constituye el núcleo de nuestro estudio, donde se evidencia la magnitud de la brecha de conocimiento y su relación con la eficiencia operativa y la exposición a vulnerabilidades. A partir de la evidencia obtenida, se establecen las implicaciones del estudio para el beneficio de la Distribuidora Leterago y se comienzan a formar ideas orientadas a responder sobre el fenómeno observado.

El capítulo V integra las conclusiones y recomendaciones derivadas del análisis. El desarrollo de este capítulo comienza a dar cierre al ciclo de congruencia vertical al responder explícitamente las preguntas de investigación y relacionarlas con la problemática inicial, formando tanto conclusiones y recomendaciones basados en los datos y su interpretación

Para finalizar, el capítulo VI, la Aplicabilidad, en él se presenta una propuesta concreta derivada de los datos, hallazgos y conclusiones del estudio. En este capítulo se desarrolla una propuesta para abordar la brecha de conocimiento identificada en la gestión de riesgos de seguridad de la información dentro de Distribuidora Leterago Honduras. También se detallan los

componentes clave de la propuesta, incluyendo su justificación, alcance, descripción y desarrollo, así como las medidas de control necesarias para su implementación. Adicionalmente, se presenta un cronograma de ejecución y un presupuesto estimado, garantizando su viabilidad operativa y económica. Finalmente, se establece la concordancia entre la propuesta y los segmentos previos de la tesis, asegurando coherencia y alineación con los objetivos de la investigación y las necesidades organizacionales identificadas.

1.2 ANTECEDENTES DEL PROBLEMA

En la actualidad, se vive un panorama en el mundo informático donde es necesario mantener estándares a los que se puede llegar por medio de la implementación de un marco de trabajo específico con el propósito de procurar la seguridad e integridad de los datos. Sin embargo, muchas personas que pertenecen a una organización o empresa omiten o desconocen la importancia de la gestión de riesgos en el área de TI.

La gestión de riesgos, declara (NIST, 2011) que:

> (…) es un proceso integral y holístico que requiere que las organizaciones: **(i) enmarquen el riesgo** (es decir, establezcan el contexto para las decisiones basadas en el riesgo); **(ii) evaluar el riesgo**; (**iii) responder al riesgo una vez determinado**; y **iv) supervisar el riesgo de forma continua** mediante comunicaciones organizativas eficaces y un ciclo de retroalimentación para la mejora continua de las actividades de las organizaciones relacionadas con el riesgo.

Para un estudio realizado entre diferentes CEOs, gerentes y jefes en puestos claves de diferentes empresas de Latinoamérica, (Pirani, 2022) asegura que “el 41,7% (de los encuestados) considera que si bien (la gestión de riesgos) es un área importante, no todos los colaboradores de la empresa la ven así y el 13% dice que es un área de poca importancia y que la mayoría no entiende cuál es su función”, lo que denota una posible brecha de conocimiento que, a largo plazo, puede ser en detrimento para el desarrollo de una organización.

En el contexto organizacional de la Distribuidora Leterago, empresa de distribución de productos farmacéuticos y, en específico, de su filial localizada en Honduras, donde se orienta a brindar soluciones tecnológicas en tareas consideradas recurrentes u operacionales principalmente a sus usuarios, luego a clientes y proveedores; se impulsa al departamento de Tecnología

Informática a ser un área **vital** para la ejecución de sus procesos operativos utilizando políticas, manuales y procedimientos que abarcan varios aspectos de la seguridad informática. Sin embargo, se encuentran brechas de conocimiento importantes como la ausencia de un modelo de gestión de riesgos de sus activos de TI orientado a la seguridad de la información, lo cual representa un riesgo significativo en su infraestructura.

Con el desarrollo de la Inteligencia Artificial y sus diferentes aplicaciones, también surge el tema de su utilización para ataques informáticos o ciberataques, ya que se han descubierto prácticas que pueden dejar expuestos los activos o la infraestructura tecnológica en general de una empresa; la adopción de la IA supera de manera masiva la supervisión y gobernanza que se ejerce para su control correcto, pues según (IBM, 2025), "el 63% de organizaciones carecen de políticas de gobierno de la IA (…) y el 62 % carece de controles de acceso adecuados en los sistemas de IA", dejando entrever que, para una variedad de empresas y rubros, la implementación de una tecnología a gestionar no tiene un control de seguimiento o una investigación preliminar para la identificación de riesgos de seguridad que pueden conllevar.

Así mismo, una de las amenazas ante las que una organización se puede ver vulnerada es el **phishing**, definido por (Dávila Angeles & Dextre Alarcón, 2021) como "una actividad maliciosa realizada por ciber atacantes que busca obtener información sensible de las víctimas", y es responsable del 16% de ataque sufridos a organizaciones por medio de hackers, suponiendo un costo promedio de 4.8 millones de dólares por cada ataque. (IBM, 2025)

(Castro Mecias, 2014) plantea que, en caso de tener una falla, ya sea en su infraestructura o software que posea la empresa, "se generan excesos de gastos en infraestructura para proteger el sistema o en tiempo y recursos del equipo de desarrollo para solucionar problemas detectados tardíamente", lo cual puede entorpecer la *eficiencia operativa general*.

Si existe una brecha de conocimiento sobre la gestión de riesgos, el área de TI de una empresa no tendrá una manera sistematizada de identificar y actuar en base a un plan de contingencia por falta de documentar incidencias, como lo disputa (INCIBE, 2015), donde "los riesgos [que] no son identificados y gestionados de forma metódica, permanecen como riesgos ocultos o no controlados" y eventualmente causar desperfectos que contribuyan a un déficit en la eficiencia operativa del área.

1.3 PLANTEAMIENTO DEL PROBLEMA

El rápido desarrollo e implementación de nuevas tecnologías de la información y la comunicación (**TIC**) en la era de la Industria 4.0, conlleva el riesgo de enfrentar brechas, vulnerabilidades y amenazas en los propios sistemas y activos tecnológicos (Putra & Soewito, 2023); mantenerse al día con los estándares en materia de seguridad de la información y ciberseguridad; más que una necesidad, es una obligación para las empresas, sean estas de menor o mayor tamaño (AL-Dosari & Fetais, 2023).

La falta de tener una gestión correcta de los riesgos en los activos de un área de TI contribuye al panorama regional de donde se desarrolla, al cambiar la ***cultura organizacional*** de una empresa influye en las demás que le rodeen dentro de la industria; "es importante que cada integrante de la organización sea consciente de los riesgos con los que conviven a diario para de esa manera poder tener más protegidos los activos", como lo plantea (Narro Mestanza, 2021), de esta manera también mitigando el riesgo de sufrir vulneraciones de datos, los cuales están valorados en promedio 4.44 millones de dólares por cada incidente. (IBM, 2025)

Añadiendo que, el desconocimiento en la priorización de riesgos y la falta de información confiable obstaculizan la toma de decisiones estratégicas y debilitan la capacidad de respuesta ante incidentes, generando también una asignación ineficiente de los recursos. **No** tener un marco definido de trabajo puede contribuir a que "las actividades de ciberseguridad (…) carezcan de una dirección estratégica clara, dificultando la integración de la ciberseguridad en la gestión de riesgos empresariales general", como lo plantea (NIST, 2024).

Todas las carencias en la mitigación de riesgos impactan negativamente en la resiliencia institucional y pueden influir en la percepción e imagen pública de esta (Beltrán Hernández et al., 2023). Por tanto, contar con una gestión **integral** de los riesgos asociados a los activos de TI no solo es una medida preventiva, sino un componente esencial para la gobernanza y la sostenibilidad organizacional.

1.4 PREGUNTAS DE INVESTIGACIÓN

1.4.1 PREGUNTA GENERAL

- ¿Cómo la (I) brecha de conocimiento existente en la gestión de riesgos de (P) la seguridad de la información del área de TI de Distribuidora Leterago, en (C) comparación con las mejores prácticas definidas en el marco normativo ISO 27005, (O) impacta en la exposición a vulnerabilidades y la eficiencia en la respuesta a

incidentes?

1.4.2 PREGUNTAS ESPECÍFICAS

- ¿De qué manera el (I) nivel de conocimiento y aplicación de las prácticas actuales de gestión de riesgos que ejecuta (P) el personal de TI de Distribuidora Leterago, en (C) comparación con los dominios de competencia definidos en ISO 27005, (O) evidencia la magnitud de la brecha de conocimiento existente?

- En (P) la estructura y cultura de Distribuidora Leterago, ¿de qué manera los (I) factores organizacionales, como la falta de políticas formales, en (C) comparación con organizaciones con una cultura de seguridad madura, (O) contribuyen a perpetuar la brecha de conocimiento en gestión de riesgos de seguridad de la información?

- ¿En qué medida los valores de indicadores operativos como el Tiempo Medio de Respuesta (I) sirven como indicadores efectivos del nivel de eficiencia operativa (O) del área de TI de Distribuidora Leterago (P) en comparación con organizaciones que tienen una cultura de seguridad madura (C), según un análisis de los datos obtenidos en los últimos 12 meses (T)?

1.5 OBJETIVOS DEL PROYECTO

1.5.1 OBJETIVO GENERAL

- Diagnosticar la brecha de conocimiento en la gestión de riesgos de la seguridad de la información dentro del área de TI de Distribuidora Leterago para determinar su impacto en la exposición a vulnerabilidades y la eficiencia operativa, (M) mediante encuestas y análisis documental de reportes de incidentes, (R) para generar un diagnóstico base que informe futuras estrategias de mitigación, (T) durante el último trimestre de 2025.

1.5.2 OBJETIVOS ESPECÍFICOS

- Determinar el nivel de conocimiento sobre gestión de riesgos de seguridad de la información en el personal de TI, (M) utilizando una matriz de competencias basada en ISO 27005 y (A) encuestas a todo el personal del área, (R) para cuantificar la brecha de habilidades, (T) en un plazo de cinco semanas.

- Identificar los factores organizacionales que perpetúan la brecha de conocimiento, (M) mediante el análisis de la documentación de políticas y (A) encuestas con los líderes de equipo, (R) para comprender las causas raíz culturales, (T) en un plazo de seis semanas.
- Determinar el nivel de eficiencia operativa por medio de la respuesta a incidentes, (M) analizando el Tiempo Medio de Respuesta (MTTR) de los (A) incidentes reportados en los últimos 12 meses, (R) para conectar la brecha de conocimiento con resultados operativos, (T) en un plazo de ocho semanas.

1.6 JUSTIFICACIÓN

Tomando en cuenta que, en una región como Latinoamérica, (Pirani, 2022) asevera que solamente para "el 43,6% de los encuestados, el área de gestión de riesgos actualmente tiene mucha importancia en sus empresas, la consideran como un área fundamental que contribuye al cumplimiento de los objetivos y a la continuidad del negocio". Siendo tan importantes los activos de TI dentro de la organización, sobre todo para el área de ventas, logística y finanzas, es necesario crear una cultura laboral donde se concientice y se priorice la gestión de riesgos para ello.

Los resultados de esta investigación buscan ser una base o instrumento para que la organización donde se desarrolle permita tener las herramientas necesarias para gestionar los riesgos de seguridad de la información del área de TI de una manera más **eficiente**, implementando nuevos **procesos** y **procedimientos** en base a un ***marco de trabajo*** ya definido. Identificar la brecha de conocimiento y saber cómo abordarla es clave para mejorar la eficiencia operativa de la organización.

European Confederation of Institutes of Internal Auditing, (2021) afirma que:

> "Las empresas que aún no han sufrido un incidente importante deben reconocer que no se trata de si los atacantes tendrán éxito, sino de cuándo. (…) El objetivo final es reducir el tiempo de inactividad y la pérdida de ingresos mientras se mantiene la confianza del cliente".

En el ámbito académico, esta investigación posee una relevancia que radica en su escasa evidencia documentada sobre implementaciones prácticas de **CVSS 4.0** en el ámbito empresarial, que, pese a ser el estándar más reciente para la evaluación de vulnerabilidades (FIRST, 2023) no

se ha encontrado una investigación en donde se especifique un caso de uso para esta herramienta, por lo cual tiene un beneficio para futuros investigadores que necesiten citar implementaciones o casos de uso.

Para poder poner en perspectiva la brecha de conocimiento, se tomará como ejemplo un elemento como la serie de actividades ejecutadas para el manejo de incidentes dentro del área de TI.

La manera en la que estos incidentes ocurridos son gestionados no solo depende del conocimiento técnico, sino de otros factores que pueden abarcar la cultura organizacional, el diseño de los procesos del área y la manera en la que opera la infraestructura. Como es posible visualizar por medio de un Diagrama de Ishikawa en la **Figura 1**, donde todos estos factores son distribuidos a lo largo de los aspectos principales o "espinas", las cuales tienen un elemento o dimensión que les pertenece, para este caso se utilizarán las dimensiones **Personas, Procesos, Políticas** y **Tecnologías**.

La dimensión de **Personas** comprende todo lo relacionado con el conocimiento y habilidades de los empleados que forman parte del manejo de incidentes; se considera que la falta de capacitación en temas o lineamientos de ciberseguridad afecta de manera que obstaculiza y estanca la eficiencia del proceso, pues estas personas toman más tiempo en procesar e identificar comportamientos o acciones que derivan en un riesgo informático.

El desconocer marcos de trabajo o normativas internacionales para la gestión de riesgos también contribuye al estancamiento de la eficiencia de este proceso; la **carencia** de herramientas técnicas y habilidades que facilitan la resolución de problemas provocan que la respuesta a incidentes no sea un proceso en el que tareas recurrentes se documenten para poder tener a mano soluciones específicas a problemas que pueden surgir con más frecuencia dentro de la infraestructura y de esta manera mitigar la exposición a vulnerabilidades futuras.

Dentro de la dimensión de **Procesos** se considera que la situación actual de la distribuidora aloja una problemática dentro de su forma de responder a incidentes al ser estas de una manera **reactiva**, significando que las acciones o decisiones que son tomadas para resolver las incidencias provienen de un resultado directo del evento ya habiendo ocurrido, sin tomar en cuenta el pensamiento a largo plazo. Para hacer una comparación, (He & Johnson, 2017) plantean que un proceso de respuesta de incidentes se debe dividir en varias fases, que incluyen la **"preparación,**

identificación, contención, erradicación, recuperación y seguimiento".

La fase final de **seguimiento** a la respuesta de incidentes se considera como "la capacidad de aprender de los errores o equivocaciones cometidos a lo largo del proceso de gestión de incidentes, conocer la eficacia de las políticas, procedimientos y procesos técnicos de seguridad y retroalimentar este conocimiento en la fase de preparación". (He & Johnson, 2017)

Este proceso definido comprende un tipo de respuesta **preventiva** o **proactiva**, donde se le da un nivel de sistematización y mejora continua a incidentes e identificación de vulnerabilidades con el propósito de contribuir a una gestión de riesgos adecuada para la escala de una organización y de esta manera, mantener un nivel constante de entrega de servicios para que las operaciones y procesos fluyan sin ningún obstáculo.

La dimensión de **Políticas** describe que no existe un **marco de trabajo** explícito, refiriéndose a que dentro de la organización la respuesta a incidentes no se rige por lineamientos y normas definidas que permitan la identificación de vulnerabilidades y mejorar la eficiencia en la respuesta, de manera que también se relaciona con la definición de una política para la prevención de riesgos informáticos. No es posible tener una política detallada para estas ocurrencias si tampoco se implementa un marco de trabajo, pues el marco es lo que da las herramientas para poder aplicarse dentro del área.

Para la dimensión de **Tecnologías**, se encuentra que la falta de documentación centralizada sobre los sistemas que maneja el área es un contribuyente directo a la eficiencia en los tiempos de respuesta a incidentes. Se plantea que las organizaciones que no tienen una manera de consultar conocimientos previos sobre el funcionamiento de un sistema o de una plataforma, ya sea por medio de una base de conocimientos o un portal de consultas, tienden a sufrir situaciones como la pérdida de conocimiento crítico (de procesos y procedimientos) así como un consumo de tiempo mayor en **buscar** el conocimiento más que en realizar funciones asignadas o desarrollando tareas que pertenecen al área, en última instancia provocando pérdidas monetarias para la organización teniendo en cuenta que existen ciertas operaciones críticas cuyo tiempo ya está medido y esperado en su ejecución. (Nakash & Bouhnik, 2020, p.8-11).

La combinación de todos estos factores dentro de las espinas contribuye de manera general a complicaciones generadas a raíz de acciones inseguras causadas por la brecha de conocimiento, conllevando tanto a la exposición de la infraestructura a vulnerabilidades, como a la reducción de

la eficiencia en tiempos de respuesta. Ver figura 1.

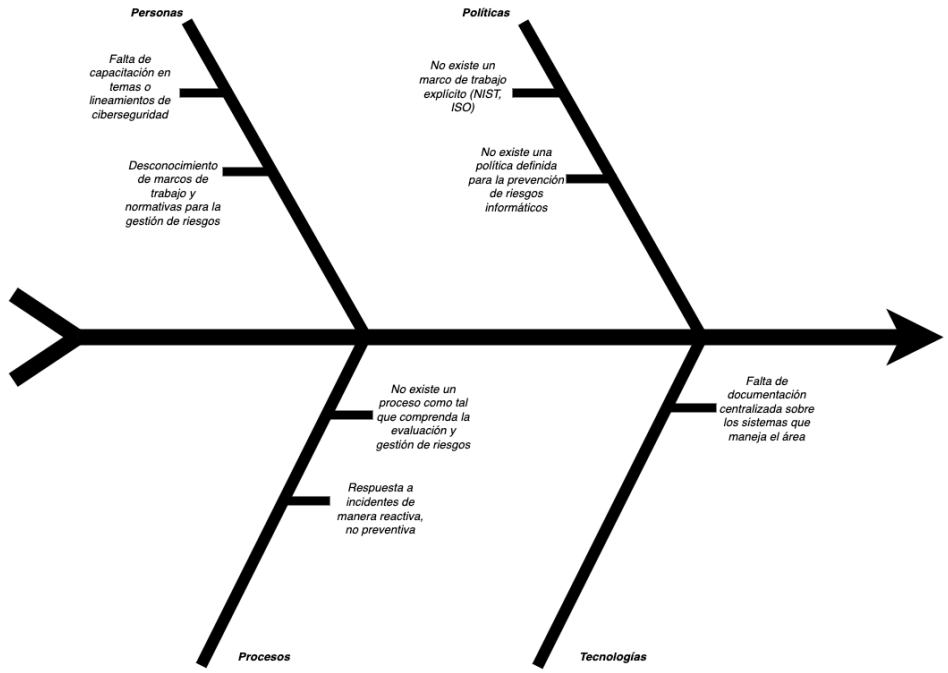


Figura 1: Diagrama de Ishikawa que analiza la exposición a vulnerabilidades y eficiencia en la respuesta a incidentes dentro del área de TI de Distribuidora Leterago.

Fuente: Elaboración propia.

CAPÍTULO II. MARCO TEÓRICO

La situación actual de la gestión de riesgos de seguridad de la información en el área de TI de la Distribuidora Leterago en Honduras refleja un panorama de vacíos estructurales y normativos que generan vulnerabilidades significativas en la gestión de riesgos de TI.

Si bien la empresa ha adoptado políticas generales de seguridad informática y cuenta con procedimientos básicos de soporte y operación, no dispone de un modelo formalizado y estandarizado de gestión de riesgos en concordancia con marcos de trabajo estandarizados. Esta carencia limita la capacidad del área de TI para identificar, evaluar, priorizar y tratar de manera sistemática los riesgos inherentes a sus activos en el aspecto de la seguridad de la información.

Este escenario evidencia una ausencia de planificación estratégica orientada a la prevención y mitigación de riesgos, lo que genera tiempos de respuesta prolongados ante incidentes de seguridad, incrementa la exposición a amenazas como el phishing, el acceso no autorizado y compromete la eficiencia operativa de procesos críticos para la organización, como la logística, la gestión financiera y en consecuencia la continuidad del negocio.

El siguiente planteamiento del marco teórico tiene como propósito retratar el estado del arte sobre la ciberseguridad y la gestión de riesgos orientada al área de TI, distribuido tanto a nivel de **macroentorno**, evaluando en diferentes aspectos países que posean un contexto socioeconómico similar, como de **microentorno,** donde se realiza una evaluación más específica a nivel de industria

2.1 ANÁLISIS DEL MACROENTORNO

Para comprender la razón por la que se desarrollan metodologías y planes de aplicación de marcos de trabajo para la gestión de riesgos, es necesario identificar leyes y normas regulativas que se apliquen a contextos similares en donde se desarrolla la investigación, como ser países en regiones que posean similares entornos al de Honduras, como ser:

- **Perú**, siempre dentro de Latinoamérica.
- **Kenia**, país dentro de la región de África Subsahariana.
- **Singapur**, país localizado en la región del sur de Asia.

Se evaluarán diferentes aspectos en base al análisis **PESTEL**, el cuál considera factores

externos que involucran el rubro en donde se desenvuelve la organización, como ser:

- **Político**
- **Económico**
- **Social**
- **Tecnológico**
- **Ecológico (o Ambiental)**
- **Legal**

Para el desarrollo de esta investigación, se considerará el factor político y legal dentro de un mismo análisis, pues las políticas desarrolladas sobre **gestión de datos, ciberseguridad y manejo de los riesgos** están fuertemente ligadas a documentos legales aprobados por los poderes **legislativos y ejecutivos** de cada país donde se realiza el análisis.

2.1.1 PERÚ

- **Político/Legal**

En Perú desde el año **2011** se implementó la **Ley de Protección de Datos Personales**, creada con el propósito de garantizar el derecho fundamental a la protección de datos personales de entidades y personas particulares almacenados en cualquier banco de datos perteneciente a una organización.

El Artículo 9 contempla que "el titular del banco de datos personales (…) debe adoptar las medidas técnicas, organizativas y legales para garantizar la seguridad de los datos personales" (CONGRESO DE LA REPÚBLICA DE PERÚ, 2011), lo cual implica que todas las organizaciones cuya información involucre datos personales de usuarios o clientes deben poseer una infraestructura tecnológica que esté construida de acorde a una normativa o estándar internacional.

La necesidad de gestionar el riesgo se vuelve imperante en este contexto y contribuye a que las organizaciones de una región tengan un nivel de estándar alto para el servicio que ofrezcan.

En esta situación, una ley sobre datos personales se convierte en un instrumento legal para que no solo las instituciones gubernamentales, sino todas las organizaciones tengan un modelo de

gestión de riesgos, alineándose posiblemente con un estándar internacional como la ISO 27005.

- **Económico**

La Unión de Telecomunicaciones Internacional (ITU, por sus siglas en inglés) es una dependencia de las Naciones Unidas creada con el propósito de fortalecer telecomunicaciones internacionales por medio de la distribución de estándares y mediciones de rendimiento.

Esta organización lanza un informe anual en el que detalla el **Índice de Ciberseguridad Global** con el propósito de medir y dar seguimiento a las diferentes políticas, leyes y cultura que se genera alrededor de la ciberseguridad en diferentes países del mundo.

Perú se encuentra en la **Categoría 3** con una puntuación de **83.74**, indicando que poseen una cultura orientada a medidas de seguridad bastante establecida dentro de su fuerza laboral, pero todavía necesitan implementar otras medidas, leyes y procesos que permitan un mejor seguimiento sobre la seguridad informática. (International Telecommunication Union (ITU), 2024).

- **Social**

La plataforma Meta comisiona una organización externa llamada Economist Impact para crear un **Índice de Inclusión al Internet,** el cual evalúa el nivel de inclusión a la sociedad con el que se integra el internet, por medio del seguimiento y evaluación de la facilidad de acceso que tiene una población hacia este servicio. (Pandey et al., 2022)

Perú se encuentra en el puesto número **42**, que, si bien significa que está desarrollando su accesibilidad, todavía se considera en crecimiento debiendo mejorar otros aspectos que conciernen a la facilidad de adquisición de dispositivos tecnológicos y educación alrededor del uso de la tecnología. (Pandey et al., 2022)

- **Tecnológico**

La Fundación de la Academia de Gobernanza Electrónica, basada en Estonia, es una organización cuya misión es “aumentar la prosperidad y la apertura de las sociedades a través de la transformación digital. (…) analizando información, se crea conocimiento sobre gobierno electrónico y transformación digital” (e-Governance Academy, 2024), para lo cual uno de sus propósitos desde 2016 fue crear el **Índice de Ciberseguridad Nacional**.

El Índice de Ciberseguridad Nacional es una herramienta para medir en tiempo real la

disponibilidad y compromiso que tiene un país ante las medidas de ciberseguridad que puede implementar. (e-Governance Academy Foundation, 2023, p.4) declara que sus hallazgos y la información que despliegan en su página web y sus reportes se basan en investigaciones sobre las capacidades operativas, legislaciones, medidas y marcos normativos que el gobierno central de un país puede implementar. Esto se monitorea por medio de diferentes áreas de capacidad que, en base a 12 indicadores, se agrupan en tres pilares principales: sus **capacidades estratégicas**, las **capacidades preventivas** y las **capacidades de respuesta** que estén relacionadas siempre al manejo de riesgos de ciberseguridad.

Tomando en cuenta estos parámetros de estudio, se encontró que, para septiembre de 2023, Perú estaba en el puesto número **53** con una puntuación de **62.34** de posibles **100**; indicadores como el de *desarrollo de políticas de ciberseguridad* o *manejo de crisis informáticas* tenían un bajo porcentaje de cumplimiento por falta de desarrollo en estas áreas. (e-Governance Academy Foundation, 2023b)

Si bien se encuentran en un **100%** de cumplimiento en indicadores como *respuestas a incidentes cibernéticos* o *protección de datos personales*, como lo mencionado en el aspecto legal, el país posee falencias suficientes como para no ser considerado con un puntaje más alto dentro del índice.

2.1.2 SINGAPUR

- **Político/Legal**

En la región sudeste del continente asiático, y, de manera más específica, en **Singapur**, desde el año 2018 existe la **Ley de Ciberseguridad**, en donde se definen medidas para la prevención, gestión y respuesta ante vulnerabilidades de índole informática dentro de las instituciones gubernamentales del país en cuestión. La ley dentro de su alcance también define lo llamado *Infraestructura Crítica de Información*, o **CII**, por sus siglas en inglés.

(REPUBLIC OF SINGAPORE, 2018, p. 14-15) define que:

> "El Comisionado puede, mediante notificación por escrito al propietario de una computadora o sistema informático, designar la computadora o el sistema informático como una infraestructura de información crítica para los fines de esta Ley, si el Comisionado está convencido de que: (a) la computadora o el sistema informático es necesario para la

prestación continua de un servicio esencial, y la pérdida o el compromiso de la computadora o el sistema informático tendrá un efecto debilitante en la disponibilidad del servicio esencial en Singapur".

Asimismo, para estas Infraestructuras Críticas de Información, dentro de la ley se establecen lineamientos para asegurar el rendimiento constante y correcto de estas tecnologías; (REPUBLIC OF SINGAPORE, 2018, p. 14-15) manteniendo que el propietario de una CII debe:

"(…) al menos una vez cada 2 años (o con la frecuencia más alta que indique el Comisionado en cualquier caso particular), a partir de la fecha de la notificación emitida en virtud de la sección 7, causar una auditoría del cumplimiento de la infraestructura de información crítica con esta Ley y los códigos de práctica y estándares de desempeño aplicables, que debe llevar a cabo un auditor aprobado o designado por el Comisionado; y (b) al menos una vez al año, a partir de la fecha del aviso emitido en virtud de la sección 7, realizar una evaluación de riesgos de ciberseguridad de la infraestructura de información crítica en la forma y manera prescritas".

Ejecutar estas tareas implica que, para garantizar el cumplimiento, los propietarios deben implementar estándares y marcos de trabajo (como ser ISO 27000 o NIST) que les permita tener gestionar y documentar los riesgos de manera sistemática y organizada.

- **Económico**

La Unión de Telecomunicaciones Internacional (ITU, por sus siglas en inglés) es una dependencia de las Naciones Unidas creada con el propósito de fortalecer telecomunicaciones internacionales por medio de la distribución de estándares y mediciones de rendimiento.

Esta organización lanza un informe anual en el que detalla el **Índice de Ciberseguridad Global** con el propósito de medir y dar seguimiento a las diferentes políticas, leyes y cultura que se genera alrededor de la ciberseguridad en diferentes países del mundo.

Singapur está en la **Categoría 1** con una puntuación de **99.86**, indicando que poseen un nivel muy alto de compromiso para coordinar esfuerzos gubernamentales y privados para mantener el cumplimiento de las medidas de seguridad informática (International Telecommunication Union (ITU), 2024).

- **Social**

La plataforma Meta comisiona una organización externa llamada Economist Impact para

crear un **Índice de Inclusión al Internet,** el cual evalúa el nivel de inclusión a la sociedad con el que se integra el internet, por medio del seguimiento y evaluación de la facilidad de acceso que tiene una población hacia este servicio. (Pandey et al., 2022)

Singapur lidera en el puesto número **1**, teniendo una puntuación perfecta en la parte técnica, considerando que su infraestructura se actualiza y mejora constantemente para mantener una alta disponibilidad y precio accesible. (Pandey et al., 2022)

- **Tecnológico**

El **Índice de Ciberseguridad Nacional,** como se menciona al estudiar el aspecto tecnológico en Perú, es una herramienta para medir en tiempo real la disponibilidad y compromiso que tiene un país ante las medidas de ciberseguridad que puede implementar (e-Governance Academy Foundation, 2023, p.4), y para el caso de Singapur, el país asiático se encuentra dentro del puesto número **31** con un puntaje de **71.43** de posibles 100. (e-Governance Academy Foundation, 2023b)

Si bien Singapur para el año 2021 tenía una calificación de **100%** en **5 de sus 12** indicadores, entre los cuales se menciona el *manejo de crisis informáticas* y *análisis de riesgos cibernéticos e informáticos*, se encontró que no existen medidas para la *protección de servicios digitales* y, si bien se han desarrollado leyes e instituciones para la *lucha contra crímenes cibernéticos*, el país no consolida del todo un sistema para poder realizar reportes en tiempo real. De igual manera, las *operaciones cibernéticas militares* incurren en una falencia, considerando que solo se han hecho ejercicios para operaciones cibernéticas, pero no existe una unidad como tal. (e-Governance Academy Foundation, 2023b)

2.1.3 KENIA

- **Político/Legal**

De manera similar, en contextos como en el que se desarrolla el país africano de Kenia, se formuló y publicó oficialmente la **Ley de Protección de Datos,** la cual establece las bases para la protección de datos personales en un entorno tecnológico cada vez más expansivo.

(REPUBLIC OF KENYA, 2019) establece que:

> "Una evaluación de impacto de la protección de datos incluirá lo siguiente: (…) una evaluación de los riesgos para los derechos y libertades de los interesados; d) las medidas

previstas para hacer frente a los riesgos y las salvaguardias, medidas de seguridad y mecanismos para garantizar la protección de los datos personales y demostrar el cumplimiento de la presente Ley, teniendo en cuenta los derechos e intereses legítimos de los interesados y otras personas interesadas."

Al mencionar en una legislación principios de seguridad y rendición de cuentas dentro de una evaluación de impacto para este aspecto de la ciberseguridad también está obligando a que una organización gubernamental o privada posean una gestión de riesgos efectiva, desde la identificación de los activos no necesariamente tecnológicos a evaluar las amenazas y daños que podrían causar, con el propósito de mantener trazabilidad e integridad de la información.

- **Económico**

La Unión de Telecomunicaciones Internacional (ITU, por sus siglas en inglés) es una dependencia de las Naciones Unidas creada con el propósito de fortalecer telecomunicaciones internacionales por medio de la distribución de estándares y mediciones de rendimiento.

Esta organización lanza un informe anual en el que detalla el **Índice de Ciberseguridad Global** con el propósito de medir y dar seguimiento a las diferentes políticas, leyes y cultura que se genera alrededor de la ciberseguridad en diferentes países del mundo.

Kenia está en la **Categoría 1** con una puntuación de **98.59**, indicando que poseen un nivel muy alto de compromiso para coordinar esfuerzos gubernamentales y privados para mantener el cumplimiento de las medidas de seguridad informática (International Telecommunication Union (ITU), 2024).

- **Social**

La plataforma Meta comisiona una organización externa llamada Economist Impact para crear un **Índice de Inclusión al Internet,** el cual evalúa el nivel de inclusión a la sociedad con el que se integra el internet, por medio del seguimiento y evaluación de la facilidad de acceso que tiene una población hacia este servicio. (Pandey et al., 2022)

Si bien Kenia es uno de los países que ha mostrado un gran avance en la facilitación del acceso a internet por medio de la creación de políticas para la implementación de la tecnología 5G, se sitúa en el puesto **58** debido a la falencia en otros aspectos de inclusión y facilidad de adquisición de dispositivos tecnológicos.

- **Tecnológico**

El **Índice de Ciberseguridad Nacional**, como se menciona al estudiar los aspectos tecnológicos en Perú y Singapur, es una herramienta para medir en tiempo real la disponibilidad y compromiso que tiene un país ante las medidas de ciberseguridad que puede implementar (e-Governance Academy Foundation, 2023, p.4), y para el caso del país subsahariano, está situado en el puesto número **86** con un puntaje de **41.56** de posibles **100**. (e-Governance Academy Foundation, 2023b)

Esto se debe a que, para el **2022**, que es donde se actualizó por última vez antes del archivado de este índice en 2023, Kenia solamente presentaba un cumplimiento del 100% en el indicador de la ***protección de datos personales***, lo cual se menciona en el aspecto político/legal, mientras que en otras áreas como ser el *manejo de crisis cibernéticas* o en el *desarrollo de políticas de ciberseguridad* estaba en falencia, obteniendo una calificación de **0%** y **43%**, de manera respectiva.

Si bien el país dentro de esos años logró un desarrollo al **67%** sobre la *educación y desarrollo profesional*, que incluye la creación de programas de ciberseguridad como carreras universitarias y maestrías dentro de instituciones públicas, no es suficiente para compensar la falta de desarrollo en sus demás indicadores. Ver tabla 1.

Tabla 1: Resumen estadístico de naciones contempladas en el macroentorno

PAÍS	RANKING EN ÍNDICE DE CIBERSEGURIDAD GLOBAL (SECTOR ECONÓMICO)	RANKING EN ÍNDICE DE INCLUSIÓN AL INTERNET (SECTOR SOCIAL)	LEGISLACIÓN RELACIONADA DIRECTA O INDIRECTAMENTE A LA GESTIÓN DE RIESGOS EN LAS ÁREAS DE TI (SECTOR POLÍTICO/LEGAL)	RANKING EN ÍNDICE DE CIBERSEGURIDAD NACIONAL (SECTOR TECNOLÓGICO)
KENIA	CATEGORÍA 1 (NIVEL ALTO DE COMPROMISO EN COORDINACIÓN GUBERNAMENTAL Y PRIVADA)	PUESTO 58	LEY DE PROTECCIÓN DE DATOS	PUESTO CON PUNTAJE DE 41.56 DE POSIBLES 100
PERÚ	CATEGORÍA 3 (CULTURA DE SEGURIDAD ESTABLECIDA EN LA FUERZA LABORAL)	PUESTO 42	LEY DE PROTECCIÓN DE DATOS PERSONALES	PUESTO CON PUNTAJE DE 62.34 DE POSIBLES 100
SINGAPUR	CATEGORÍA 1 (NIVEL ALTO DE COMPROMISO EN COORDINACIÓN GUBERNAMENTAL Y PRIVADA)	PUESTO 1	LEY DE CIBERSEGURIDAD	PUESTO CON PUNTAJE DE 71.43 DE POSIBLES 100

Fuente: Elaboración propia con data de (e-Governance Academy Foundation, 2023b), (International Telecommunication Union (ITU), 2024) y (Pandey et al., 2022).

2.2 ANÁLISIS DEL MICROENTORNO

Además de compartir fronteras y un trasfondo cultural casi calcado con el resto de los países del istmo centroamericano como Guatemala, El Salvador, Nicaragua, Costa Rica y Panamá, estos países poseen un contexto muy similar al nuestro en Honduras, sin embargo, en materia de vinculación de la gestión de riegos de TI y su adopción en las empresas, realizando una búsqueda más profundidad, es notable que se carece de documentación o publicación sobre la temática para el caso de este país, no así para el resto de la región.

Fuerza competitiva centroamericana en la importación y exportación medicamentos

Tabla 2: Análisis de Importaciones y Exportaciones de Medicamentos en Centroamérica para 2024.

ANALISIS CENTROAMERICANO DEL MERCADO FARMACEUTICO

IMPORTACIONES DE MEDICAMENTOS 2024 (Millones de US$)

	GUATEMALA	EL SALVADOR	NICARAGUA	COSTA RICA	PANAMÁ	HONDURAS
EXTRAREGIONAL	835.6	476	332.1	639.6	639	434.6
INTRAREGIONAL	71.9	77.8	137.6	94.1	34.3	225.8

TOTAL, IMPORTACIONES CUARTO TRIMESTRE 2024 (MEDICAMENTOS - Porcentaje %)

	GUATEMALA	EL SALVADOR	NICARAGUA	COSTA RICA	PANAMÁ	HONDURAS
EXTRAREGIONAL	NA	3.7	4	NA	4.9	NA
INTRAREGIONAL	NA	NA	4.4	6	NA	6.6

EXPORTACIONES DE MEDICAMENTOS 2024 (Millones de US$)

	GUATEMALA	EL SALVADOR	NICARAGUA	COSTA RICA	PANAMÁ	HONDURAS
EXTRAREGIONAL	42.7	31.8	NA	NA	29	NA
INTRAREGIONAL	352.9	141	NA	125.7	2.2	45

TOTAL, EXPORTACIONES CUARTO TRIMESTRE 2024 (MEDICAMENTOS - Porcentaje %)

	GUATEMALA	EL SALVADOR	NICARAGUA	COSTA RICA	PANAMÁ	HONDURAS
EXTRAREGIONAL	NA	NA	NA	NA	NA	NA
INTRAREGIONAL	6.5	4.2	NA	NA	NA	NA

Fuente: Elaboración propia, con data de Sistema de Estadísticas de Comercio de Centroamérica (SIECA, 2025a, 2025b)

Es importante reconocer que es mucho más común encontrar información sobre empresas de la región que ha adoptado la norma **ISO 27001** en sus operaciones de TI, la que funge como un estándar para la seguridad de la información, y no específicamente sobre la norma bajo la ISO 27005, que se especializa en la gestión de riesgos de TI, y aún menos documentada se encuentra la adopción de los marcos de trabajo **NIST SP 800-53** o **NIST SP 800-30**.

Este fenómeno es digno de someterse a estudio, pues podría tratarse de una baja adopción o interés sobre el tema de gestión de riesgos de TI, o simplemente un tema de hermetismo organizacional en donde se restringe compartir esta información.

Se introduce como ejemplo práctico la industria en Guatemala y se culmina con un análisis

de la situación para Distribuidora Leterago en Honduras.

Guatemala

- **Rivalidad entre Competidores:** Alta. Varias distribuidoras con fuerte capital compiten agresivamente, utilizando plataformas digitales para pedidos y seguimiento de stock. La seguridad de TI comienza a ser un diferenciador, especialmente en el manejo de datos sensibles de clientes.
- **Amenaza de Nuevos Entrantes:** Moderada. El mercado es atractivo para cadenas distribuidoras que buscan integrar la distribución con farmacias propias. El reto principal es cumplir con regulaciones sanitarias y contar con infraestructura tecnológica segura.
- **Poder de Negociación de los Proveedores:** Alto. Los laboratorios multinacionales dominan y fijan condiciones, incluyendo requerimientos tecnológicos en trazabilidad y auditoría de datos.
- **Poder de Negociación de los Clientes:** Dual. Los grandes hospitales y farmacias corporativas exigen sistemas de gestión robustos y reportes confiables, mientras que las farmacias pequeñas priorizan precio y disponibilidad.
- **Amenaza de Sustitutos:** Creciente. El auge de plataformas digitales de salud y farmacias online puede reducir la dependencia del distribuidor tradicional, exigiendo mayores inversiones en TI y seguridad.

2.3 CONCEPTUALIZACIÓN

Dentro de la investigación, es necesario sentar las bases de los términos que se verán utilizados con más frecuencia por los documentos que se están citando y por el uso que den los mismos autores de ella, con el propósito de facilitar la comprensión de este documento.

1. Tecnologías de la Información (TI).

De acuerdo con (Colman, 2009), se puede definir las **Tecnologías de la Información** como el "uso o estudio de computadores, sistemas de telecomunicación y otros dispositivos para crear, procesar, almacenar y transferir información". Esto implica que dispositivos como televisores o redes de telecomunicación se incluyen dentro de esa categoría.

En el caso de esta investigación, es el campo que se tomará en cuenta para evaluar la brecha de conocimiento sobre la gestión de riesgos.

2. Activo de TI.

"Un **activo** es un recurso de propiedad o controlado por un negocio o una entidad económica. Es todo aquello tangible o intangible que puede ser utilizado para producir valor" (O'Sullivan & Sheffrin, 2004), y para el caso de la investigación se toma en cuenta la dimensión de TI, que conlleva todo lo tecnológico que es utilizado para para producir valor, dentro de lo que se considera para comprender como se evalúan los riesgos.

3. Riesgo informático.

El **riesgo informático**, definido por (NIST, 2011) como "el riesgo asociado con la operación y el uso de los sistemas de información que respaldan las misiones y las funciones operativas de sus organizaciones", es pertinente para la investigación el motivo de ser un elemento que se evalúa dentro de la gestión.

4. Ciberataque.

Un **ciberataque** es una acción deliberada y malintencionada, ejecutada por un actor de amenazas (individuo, grupo u organización) con el objetivo de comprometer la confidencialidad, integridad o disponibilidad de los sistemas de información, redes o datos de una víctima. (McCarthy et al., 2023). Se considera importante para la comprensión de la investigación debido a que es una de las acciones que pueden ocurrir en un entorno tecnológico cuyo valor de los datos sea crítico y se debe tomar en cuenta para una gestión de riesgos eficiente.

5. Ciberseguridad.

Definido como "la capacidad de proteger o defender el uso del ciberespacio de los ataques cibernéticos" (McCarthy et al., 2023), es uno de los pilares para el entendimiento de un plan de gestión de riesgos para el área de TI, pues forma parte de los aspectos más importantes para ello, como ser el tomar medidas, implementar acciones recurrentes o configuraciones dentro de una infraestructura tecnológica.

6. Ciberespacio.

(NIST, 2011) lo define como "un dominio global dentro del entorno de la información que

consiste en la red interdependiente de infraestructuras de sistemas de información, incluyendo Internet, redes de telecomunicaciones, sistemas informáticos y procesadores y controladores integrados"; para el caso de esta investigación se considera importante comprender como éste es el ambiente externo para el cual se desarrollan planes de gestión de riesgos orientadas al área de TI. El ciberespacio es aquello que rodea y con lo que los activos del área interactúan; la gestión de riesgos limita lo que se puede hacer de cara al dominio global.

7. Marco de trabajo.

Un **marco de trabajo** (framework) es "una estructura conceptual o real que proporciona un conjunto de mejores prácticas, estándares, guidelines y procesos estandarizados diseñados para ayudar a las organizaciones a gestionar y alinear sus actividades con los objetivos estratégicos", como lo plantea (ISACA, 2012), para lo cual dentro de la investigación esto proporciona una base sistemática para la gestión de riesgos.

8. Eficiencia operativa.

Cuando se habla de **eficiencia operativa**, (Brandon-Jones & Slack, 2019) declara que es "la capacidad de una organización para entregar productos o servicios de la manera más económica posible, optimizando el uso de sus recursos (tiempo, dinero, personal) sin comprometer la calidad", dentro de la investigación se relaciona hacia la gestión de riesgos por ser uno de los motivadores más importantes para el desarrollo de planes y el esfuerzo de entender y formular medidas para atacar la brecha de conocimientos. Mientras más se comprenda la importancia de la gestión de riesgos, más se apunta a mantener y mejorar la eficiencia operativa no sólo del área de TI, sino todas las áreas que interactúan con ella.

9. Gestión de Riesgos.

(NIST, 2011) define la **gestión de riesgos** como:

> "(…) un proceso integral que requiere que las organizaciones: (i) **enmarquen el riesgo** (es decir, establezcan el contexto para las decisiones basadas en el riesgo); (ii) **evaluar el riesgo**; (iii) **responder al riesgo una vez determinado**; y iv) **supervisar el riesgo** de forma continua mediante comunicaciones institucionales eficaces y un ciclo de retroalimentación para la mejora continua de las actividades de las organizaciones relacionadas con el riesgo (…) se lleva a cabo como una actividad holística en toda la organización que aborda el

riesgo desde el nivel estratégico hasta el nivel táctico, asegurando que la toma de decisiones basada en el riesgo se integre en todos los aspectos de la organización".

En el caso de la investigación, es el tema principal sobre el que se quiere analizar la brecha de conocimientos dentro del área de TI.

10. Política de Seguridad Informática.

"Una **política de seguridad** es un conjunto de criterios para la prestación de servicios de seguridad", según (NIST, 2011), tomando en cuenta que es uno de los objetos a desarrollar dentro de la gestión de riesgos y el instrumento que permite poner de manera oficial el proceder de un área o de una empresa para la previsión o la actuación sobre procedimientos o acciones inseguras que puedan desestabilizar una infraestructura informática.

11. Infraestructura Tecnológica.

La manera en la que define (Tassey, 1992) la **Infraestructura Tecnológica** es como "el conjunto de componentes (…) interconectados (como computadoras, servidores, dispositivos de red, sistemas operativos, bases de datos y aplicaciones empresariales) que proporcionan la base fundamental para soportar las operaciones, la entrega de servicios y las aplicaciones de una organización". Para el desarrollo de la investigación, se considera pertinente la infraestructura tecnológica debido a que es el objeto de estudio y aplicación de la gestión de riesgos para una empresa.

12. Tiempo Medio de Respuesta.

El **Tiempo Medio de Respuesta** o **MTTR,** por sus siglas en inglés, es "una métrica clave de seguridad que calcula el tiempo promedio que tarda un equipo o área de TI en contener y/o mitigar un incidente de seguridad informática después de que se ha detectado", según (Cichonski et al., 2012).

Para motivos de la investigación se toma en cuenta con el motivo de hacer un análisis sobre el efecto que tiene realizar labores del área de TI sin un marco de trabajo definido y como puede afectar a esta métrica.

13. Seguridad de la Información.

De acuerdo con (International Organization for Standardization (ISO), 2018), la seguridad

de la información corresponde a la "preservación de la **confidencialidad**, **integridad** y **alta disponibilidad** de la información".

14. Riesgo de Seguridad de la Información.

Un riesgo de seguridad de la información se considera como "el efecto de la **incertidumbre** sobre los objetivos de la seguridad de la información", según (International Organization for Standardization (ISO), 2018)**.**

15. ISO 27005.

La ISO 27005 es una normativa, actualizada por última vez en 2022, que, planteada por (International Organization for Standardization (ISO), 2022) y tiene el propósito de "proveer una guía para la implementación de los requerimientos para gestionar el riesgo de seguridad de la información", así como "acciones que tomar para la gestión de riesgos de seguridad de la información".

2.4 TEORÍAS DE SUSTENTO

Para poder desarrollar una investigación que sea contemplada como un documento con datos verídicos y bases teóricas sólidas es necesario poder relacionarla con teorías que contemplen el contexto, dinámicas y comportamientos de la organización.

2.4.1 BASES TEÓRICAS

La **Teoría de la Agencia**, que por nombre completo lleva ***Teoría del Agente-Principal***, es lo que se refiere a la explicación de comportamientos y conflictos de interés que surgen en una interacción frecuente. El enfoque de la teoría del agente-principal es determinar el funcionamiento óptimo de un contrato social u operativo, en donde se describe el comportamiento contra el resultado (Eisenhardt, 1989).

Existe un modelo simple, en donde se asume que existe un conflicto de metas e intereses entre un "**agente**" y un "**principal**"; el principal es aquella persona o entidad que implica una diferencia de poder entre él y su "agente", aquella persona o entidad que sirve como ejecutora de tareas para el cumplimiento de metas del "principal". Este conflicto de intereses surge a raíz de que "el principal y el agente tienen metas no alineadas y (…) el principal no puede determinar si el comportamiento del agente es el correcto al ejecutar las tareas". (Eisenhardt, 1989)

En el caso de esta investigación se puede interpretar que el "**principal**" corresponde a la ***alta dirección de la Distribuidora Leterago*** y el "**agente**" como ***el área de TI***; en este caso, la Alta Dirección es posible que no pueda evaluar por sí solo el riesgo que conlleva manejar el área de TI por diversas razones (falta de conocimiento técnico, poca familiarización con políticas tecnológicas) y el área de TI no tiene el suficiente apoyo dentro de la cultura organizacional para implementar un marco de trabajo.

La **Teoría del Aprendizaje Organizacional**, en cambio, estudia la manera en la que las organizaciones *formulan, preservan y trasmiten* el conocimiento a lo largo de la cadena jerárquica de sus empleados.

Se plantea la existencia de varios tipos de aprendizaje dentro de las organizaciones, donde el *aprendizaje de bucle simple*, según (Fiol & Lyles, 1985), "[es] el proceso que mantiene las características principales de la teoría en uso o reglas establecidas de una organización y se restringe a detectar y corregir errores dentro de ese mismo juego de reglas", mientras que el *aprendizaje avanzado* o, mejor llamado, *bucle doble*, es el que "apunta a hacer ajustes de las reglas o crear nuevas en vez de realizar siempre actividades o comportamientos que se limiten a un universo definido". (Fiol & Lyles, 1985)

Dentro de esta teoría se puede adaptar en el sentido en que, para comprender una gestión de riesgos efectiva, es necesario que la organización funcione con un aprendizaje de bucle doble, pues siempre es necesario mantener un enfoque de mejora continua de sus políticas en un entorno cambiante como es el de las tecnologías de la información.

Esta manera de operar solo puede realizarse de una manera efectiva y congruente por medio de la socialización y gestión correcta del conocimiento que se considera de uso colectivo para una organización y de esta manera apuntando a comprender como atacar una brecha de conocimiento sobre cualquier tema de alta importancia, en este caso, la *gestión de riesgos para los activos en el área de TI.*

2.5 ANÁLISIS DE LAS METODOLOGÍAS

El diseño metodológico de esta investigación se construirá sobre un esquema de coherencia vertical que garantiza la alineación entre el problema identificado, las preguntas de investigación, los objetivos planteados y las herramientas a utilizar. (Hernández Sampieri & Mendoza Torres,

2018) indica que el planteamiento del problema y su contexto provee una base para la cual se elige una metodología en específico, ya sea ***cualitativa, cuantitativa*** o ***mixta***.

Esto depende de la visión del investigador ante lo que quiere obtener del tipo de fenómeno estudiado, así como tiempo y recursos disponibles y, si bien los tres componen las mismas estrategias generales, su proceder y características pueden ser diferentes de manera específica.

Para mostrar la información de la coherencia vertical se realiza una **matriz de coherencia vertical**, ver tabla 3; entro de la cual se "incluye un conjunto de indicadores y fuentes de verificación (en particular para los fines y los resultados), que permitirán recopilar y utilizar la información de gestión de manera oportuna y rentable", según lo mencionado por (European Commission, 2004). Para adaptarlo al desarrollo de la investigación, se tomará en cuenta que los elementos a investigar provienen del Capítulo 1, donde se plantea el problema, las preguntas y objetivos de investigación, dentro de los cuales se evalúa cuál es su componente principal, como se analizará este de manera metodológica y, principalmente, **cuál** es la finalidad de hacer este análisis.

2.5.1 MATRIZ DE COHERENCIA VERTICAL

Tabla 3. Vinculación Metodología – Elementos clave de la investigación

ELEMENTO PARA INVESTIGAR	COMPONENTE	INSTRUMENTO METODOLÓGICO DE ANÁLISIS O CAPTURA	FINALIDAD
PROBLEMA GENERAL	Brecha de conocimiento sobre la gestión de riesgos que desemboca en efectos negativos hacia la eficiencia operativa y vulnerabilidades en la infraestructura.	Estrategia de Triangulación: estudio de evidencia objetiva y métricas cuantitativas sobre percepciones subjetivas.	Diagnosticar de manera integral y holística el impacto de la brecha de conocimientos.
PREGUNTA GENERAL	¿Cómo la brecha de conocimiento existente en gestión de riesgos de la seguridad de la información en el área de TI de Distribuidora Leterago, en comparación con las mejores prácticas definidas en el marco normativo ISO 27005, impacta en la exposición a vulnerabilidades y la eficiencia en la respuesta a incidentes?	Estudio de Caso Único.	Profundizar en el "por qué" y el "cómo" dentro del contexto organizacional.

ELEMENTO PARA INVESTIGAR	COMPONENTE	INSTRUMENTO METODOLÓGICO DE ANÁLISIS O CAPTURA	FINALIDAD
OBJETIVO GENERAL	Diagnosticar la brecha de conocimiento en la gestión de riesgos de la seguridad de la información dentro del área de TI de Distribuidora Leterago para determinar su impacto en la exposición a vulnerabilidades y la eficiencia operativa, mediante encuestas y análisis documental de reportes de incidentes, para generar un diagnóstico base que informe futuras estrategias de mitigación, durante el último trimestre de 2025.	Diseño Secuencial Exploratorio	Explorar la problemática de manera *cualitativa*, así como evaluar aspectos clave (métricas) de manera *cuantitativa*
PREGUNTA ESPECÍFICA 1	¿De qué manera el nivel de conocimiento y aplicación de las prácticas actuales de gestión de riesgos que ejecuta el personal de TI de Distribuidora Leterago, en comparación con los dominios de competencia definidos en ISO 27005, evidencia la magnitud de la brecha de conocimiento existente?	Matriz de Evaluación de Competencias basado en el dominio definido por la norma ISO 27005. Encuestas.	Cuantificar y cualificar la brecha de conocimientos y competencias.
OBJETIVO ESPECÍFICO 1	Determinar el nivel de conocimiento sobre gestión de riesgos de la seguridad de la información en el personal de TI, utilizando una matriz de competencias basada en ISO 27005 y encuestas a todo el personal del área, para cuantificar la brecha de habilidades, en un plazo de cinco semanas.	Análisis de los resultados de las encuestas y valoración de la Matriz de Evaluación de Competencias.	Obtener una medición preliminar sobre lo considerado como “conocimiento”.

ELEMENTO PARA INVESTIGAR	COMPONENTE	INSTRUMENTO METODOLÓGICO DE ANÁLISIS O CAPTURA	FINALIDAD
PREGUNTA ESPECÍFICA 2	En la estructura y cultura de Distribuidora Leterago, ¿de qué manera los factores organizacionales, como la falta de políticas formales, en comparación con organizaciones con una cultura de seguridad madura, contribuyen a perpetuar la brecha de conocimiento en gestión de riesgos?	Análisis de documentación, incluyendo políticas vigentes o históricas.	Identificación de causas raíz dentro del contexto de la cultura organizacional y estructural.
OBJETIVO ESPECÍFICO 2	Identificar los factores organizacionales que perpetúan la brecha de conocimiento, mediante el análisis de la documentación de políticas y encuestas con los líderes de equipo, para comprender las causas raíz culturales, en un plazo de seis semanas.	Análisis del contenido de la documentación.	Identificación de respuestas relacionadas (patrones, temáticas similares) al desenvolvimiento de la cultura organizacional.
PREGUNTA ESPECÍFICA 3	¿Cómo la ausencia de un marco formal para el proceso de respuesta a incidentes ocurridos dentro de la Distribuidora Leterago, en comparación con un proceso basado en guías del NIST o ISO, impacta la eficiencia en la identificación, priorización y tratamiento de amenazas a los activos de TI?	Análisis de datos históricos sobre incidentes y respuestas a los incidentes (métricas cuantificables como el MTTR).	Relacionar la brecha de conocimiento con datos tangibles.
OBJETIVO ESPECÍFICO 3	Evaluar el impacto de la ausencia de un marco formal por medio de la eficiencia de la respuesta a incidentes, analizando el Tiempo Medio de Respuesta (MTTR) de los incidentes reportados en los últimos 12 meses, para conectar la brecha de conocimiento con resultados operativos, en un plazo de ocho semanas.	Análisis estadístico descriptivo en base a series de tiempo (interpretación de los datos obtenidos a lo largo de un periodo de tiempo definido).	Establecer una base en la que se sitúa el desempeño operativo actual del área.

Fuente: Elaboración propia

2.5.1 DECLARACIÓN DE REFLEXIVIDAD

Como grupo de investigadores dentro de los cuales uno de ellos labora en la empresa al momento de realizar la investigación, se deben tomar en cuentas varios factores que pueden afectar la investigación o cambiar el rumbo del enfoque seleccionado.

Al poseer acceso privilegiado a los datos de la empresa con una autorización firmada previamente, existe no solo un riesgo de filtración de información considerada sensible, ya sea voluntaria o involuntariamente, sino el de un posible sesgo de confirmación proveniente de la interpretación de los datos para efecto de confirmar las observaciones que fueron planteadas como la problemática general.

La manera de mitigar este riesgo es aplicando una estrategia de triangulación en la que las **percepciones subjetivas**, como ser encuestas o encuestas a las personas del área de TI se ponen en comparación o se analizan de manera paralela a la **evidencia objetiva** que se encuentre, esto puede incluir políticas de la empresa o reportes sobre riesgos informáticos hasta las **métricas cuantitativas** que se están considerando para los objetivos específicos, como ser el MTTR.

2.5.2 ESTRATEGIA DE TRIANGULACIÓN

Según (Denzin, 1978) se define la triangulación como "la aplicación y combinación de varias metodologías de la investigación en el estudio de un mismo fenómeno", por lo que si se considera la palabra "estrategia" dentro de este contexto se puede definir como un plan estructurado para aplicar y combinar diferentes metodologías. Una estrategia se puede descomponer en varios temas que se relacionan para obtener un resultado más homogéneo, como ser:

- **Triangulación de Datos**

La triangulación de los datos comprende "(…) a la **utilización de diferentes estrategias y fuentes de información** sobre una recogida de datos [que] permite contrastar la información recabada", como lo plantea (Aguilar Gavira & Barroso Osuna, 2015).

Dentro de la investigación se recopilará información que provienen de diferentes lugares, como ser el **personal técnico de TI**, **líderes de equipo**, **documentación interna** y **registros históricos de incidentes**.

- **Triangulación Metodológica**

La triangulación metodológica se define como "la **aplicación de diversos métodos** en la misma investigación para recaudar información contrastando los resultados, analizando coincidencias y diferencias" (Aguilar Gavira & Barroso Osuna, 2015).

Para el caso de la investigación a desarrollar se interpretaría con el propósito de emplear métodos **cualitativos** (encuestas, análisis documental de las políticas) y **cuantitativos** (análisis de métrica MTTR, matriz de evaluación de competencias basada en ISO 27005) para obtener una visión completa y contextualizada del problema.

- **Triangulación Teórica**

Se puede considerar triangulación teórica como un método que "hace referencia a la utilización de distintas teorías para tener una interpretación más completa y comprensiva, y así dar respuesta al objeto de estudio, pudiendo incluso ser estas teorías antagónicas" (Aguilar Gavira & Barroso Osuna, 2015), y para el caso de esta investigación se tratará de contrastar los hallazgos empíricos con los marcos teóricos de la **Teoría de la Agencia** y el **Aprendizaje Organizacional**, así como con los estándares normativos (**ISO 27005, NIST**).

2.5.3 HERRAMIENTAS DE ANÁLISIS METODOLÓGICO

Con el motivo de homogeneizar la manera de aplicar análisis a situaciones, resultados de instrumentos de recolección de datos y darles contexto, se utilizarán diferentes herramientas de análisis metodológico; los diagramas de Ishikawa, las matrices de codificación para evaluación de competencias y diagramas o gráficos de series de tiempo se incluyen por diferentes motivos que son explicados más a fondo en cada una de las entradas.

- **Diagramas de Ishikawa**

Permitirá visualizar las relaciones entre las dimensiones organizacionales identificadas **(Personas, Procesos, Políticas, Tecnología)** y como estas ejercen un impacto en la brecha de conocimiento y la eficiencia operativa.

- **Matrices de Codificación**

Se utilizarán con el propósito de organizar sistemáticamente los temas que surjan del análisis temático de las encuestas, permitiendo evaluar la brecha de conocimientos y competencias,

así como mantener una trazabilidad clara desde los datos crudos hasta las conclusiones.

- **Diagramas de Series de Tiempo**

Se utilizarán para retratar las gráficas que evalúen la evolución de la métrica MTTR a lo largo del período de análisis, facilitando la identificación de patrones y correlacionar eventos específicos con el contexto general de la organización y como esto concierne al desarrollo de la investigación.

2.6 ANTECEDENTES DE LAS METODOLOGÍAS

Tradicionalmente, la investigación en temas relacionados a Tecnologías de la Información y ciberseguridad se ha inclinado por estudios cuantitativos a gran escala que buscan generalizar hallazgos o diseños experimentales altamente controlados, a menudo descontextualizados de la realidad organizacional compleja y dinámica.

Esta investigación adopta en cambio un enfoque práctico y reflexivo alineado con la tradición de los estudios de caso en sistemas de información.

La propuesta metodológica captura tanto la profundidad contextual **(cualitativa)** como la evidencia métrica tangible **(cuantitativa)**, ofreciendo una visión holística e integral que los enfoques tradicionales puros no pueden alcanzar.

2.7 METODOLOGÍAS, ENFOQUES, MÉTODOS, DISEÑOS

La presente investigación adopta un **enfoque mixto** definido como "una representación de un conjunto de procesos sistemáticos, empíricos y críticos de investigación que implican la recolección y el análisis de datos cuantitativos y cualitativos, así como su integración y discusión conjunta, para realizar inferencias producto de toda la información recabada (meta inferencias) y lograr un mayor entendimiento del fenómeno bajo estudio" (Hernández Sampieri & Mendoza Torres, 2018, p. 612)

Como el enfoque mixto resulta más propio para esta investigación, significa que puede ser considerada una investigación multimetódica, ver figura 2 para visualizar dónde se sitúa a los métodos mixtos dentro del espectro de las clases de investigación y diseños en la tipología de diseños.

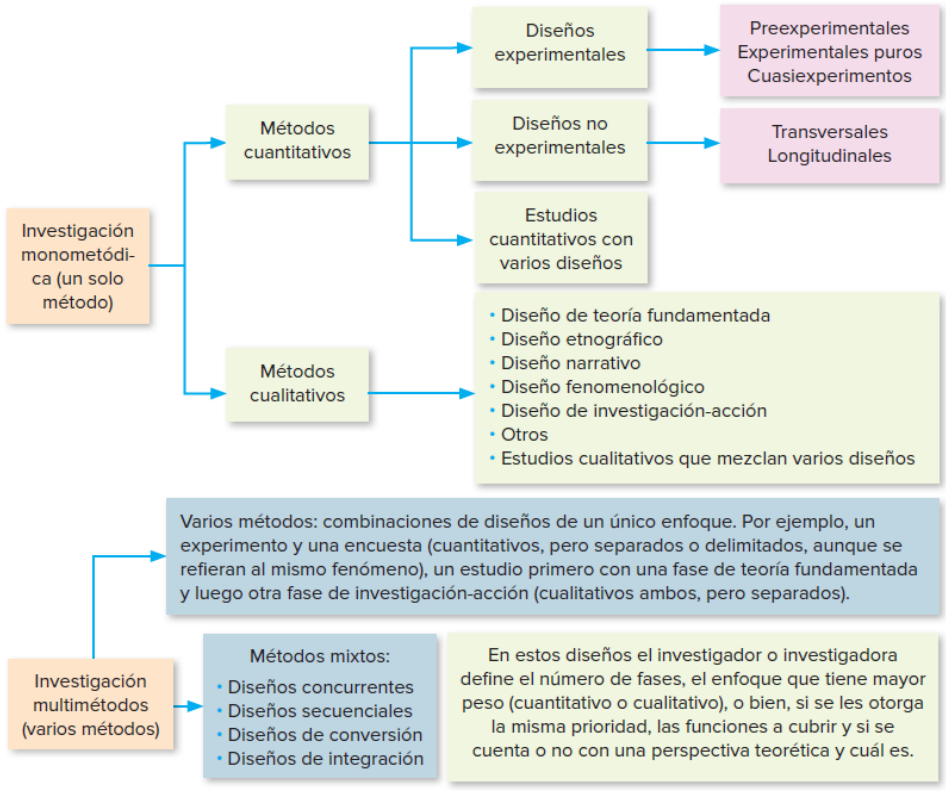


Figura 2. Métodos mixtos dentro del panorama o espectro de la investigación

Fuente: (Hernández Sampieri & Mendoza Torres, 2018, p. 613)

Basándose en la información plasmada en la tabla 4, el siguiente paso sería seleccionar el tipo de diseño que mejor se ajuste al proceso de recolección y análisis de información, y para ello es necesario tomar en cuenta algunas consideraciones.

Tabla 4. Elementos para decidir el diseño general apropiado en una investigación de enfoque mixto

Tiempos	Prioridad o peso	Mezcla más común	Teorización
Concurrente (no hay secuencia)	Igual	Integrar ambos métodos	Explícita
Secuencial: primero el método cualitativo	Cualitativo (CUAL)	Conectar un método con el otro	Implícita
Secuencial: primero el método cuantitativo	Cuantitativo (CUAN)	Anidar o incrustar un método dentro de otro	

Fuente: (Hernández Sampieri & Mendoza Torres, 2018, p. 630)

Teniendo claro que se trata de una investigación con enfoque mixto, se cuenta con diferentes opciones de diseño, así mostrado en la tabla 5; se selecciona el **Diseño Exploratorio Secuencial** (DEXPLOS) por su ventaja relativa de mayor facilidad de implementación, con etapas claras y marcadas.

La Fase 1 **(cualitativa)** permite utilizar encuestas, análisis documental y permitirá diagnosticar la brecha de conocimiento, comprender sus causas y definir los parámetros clave.

La Fase 2 **(cuantitativa)** en donde se puede analizar métricas, y datos estadísticos, se nutrirá de los hallazgos de la primera para cuantificar el impacto operativo y la magnitud de la brecha de habilidades, permitiendo una conexión robusta entre las percepciones cualitativas y los resultados medibles.

Tabla 5. Tipos de Diseño para enfoque mixto

Nombre del Diseño	Descripción General	Prioridad/Peso	Propósito Principal de la Integración
1. Diseño Exploratorio Secuencial (DEXPLOS)	Implica una fase inicial de recolección y análisis de datos cualitativos, seguida de una fase donde se recaban y analizan datos cuantitativos. La fase cuantitativa se basa en los resultados cualitativos.	Comúnmente cualitativa (CUAL), aunque puede ser cuantitativa (CUAN) si el estudio busca enfocarse principalmente en CUAN, pero necesita datos CUAL iniciales.	Exploración inicial del planteamiento, probar elementos de una teoría emergente (de la fase CUAL) y generalizarla, desarrollar un instrumento estandarizado, o determinar la distribución de un fenómeno.

Nombre del Diseño	Descripción General	Prioridad/Peso	Propósito Principal de la Integración
2. Diseño Explicativo Secuencial (DEXPLIS)	Se caracteriza por una primera etapa de recolección y análisis de datos cuantitativos, seguida de otra donde se recogen y evalúan datos cualitativos. La fase cualitativa se construye sobre los resultados cuantitativos iniciales.	Comúnmente cuantitativa (CUAN), aunque puede ser cualitativa (CUAL) para caracterizar casos.	Utilizar resultados cualitativos para auxiliar en la interpretación y explicación de los descubrimientos cuantitativos iniciales, profundizando en ellos, o cuando aparecen resultados cuantitativos inesperados o confusos.
3. Diseño Transformativo Secuencial (DITRAS)	Incluye dos etapas de recolección de datos (CUAN y CUAL), guiado por una perspectiva teórica amplia (teorización, ej., feminismo, acción participativa) que es más importante que el método en sí. Los resultados se integran durante la interpretación.	Puede ser CUAN o CUAL o igual, pero la perspectiva teórica es la guía principal.	Emplear los métodos más útiles para la perspectiva teórica, involucrar a los participantes con mayor profundidad, o entender el fenómeno bajo uno o más marcos de referencia transformativos.
4. Diseño de Triangulación Concurrente (DITRIAC)	Recolección y análisis simultáneo de datos cuantitativos y cualitativos sobre el problema de investigación. La interpretación y discusión explican las dos clases de resultados, generalmente	Puede darse prioridad a CUAN, CUAL o igual peso.	Confirmar o corroborar resultados, efectuar validación cruzada entre datos cuantitativos y cualitativos, aprovechar las ventajas de cada método y minimizar sus debilidades.

Nombre del Diseño	Descripción General	Prioridad/Peso	Propósito Principal de la Integración
	comparando las bases de datos "lado a lado".		
5. Diseño Anidado o Incrustado Concurrente de Modelo Dominante (DIAC)	Colecta simultáneamente datos cuantitativos y cualitativos, pero un método predominante guía el proyecto (CUAN o CUAL). El método con menor prioridad es anidado o insertado dentro del que se considera central.	Dominante: CUAN o CUAL; el otro es secundario (minúscula).	Proporcionar distintas visiones del problema; por ejemplo, datos CUAN para efectos de tratamientos y evidencia CUAL para explorar vivencias de participantes.
6. Diseño Anidado Concurrente de Varios Niveles (DIACNIV)	Recolección de datos cuantitativos y cualitativos en diferentes niveles de análisis (ej., individuos, grupos, organizaciones). Los análisis pueden variar en cada uno de estos niveles.	No se especifica una prioridad general, ya que puede variar por nivel o enfoque.	Buscar información en diferentes grupos o niveles de análisis para una comprensión más completa y multifacética del fenómeno.
7. Diseño	Conjunta elementos de	Puede darse o no mayor peso	Hacer converger la

Nombre del Diseño	Descripción General	Prioridad/Peso	Propósito Principal de la Integración
Transformativo Concurrente (DISTRAC)	modelos previos: recolección de datos cuantitativos y cualitativos en un mismo momento (concurrente), guiado por una teoría, visión, ideología o perspectiva (como en el DITRAS). Puede adquirir formato anidado o de triangulación.	a un método, pero la teoría o marco de referencia es fundamental.	información cuantitativa y cualitativa, ya sea anidándola, conectándola o haciéndola confluir, siempre bajo la guía de un marco teórico transformativo.
8. Diseño de Integración Múltiple (DIM)	Implica la mezcla más completa y sumamente itinerante de métodos cuantitativos y cualitativos. Ambas aproximaciones se entremezclan desde el inicio hasta el final, o al menos en la mayoría de sus etapas.	Sugiere un peso equilibrado o interdependencia constante de ambos enfoques a lo largo de todo el proceso.	Liderar con problemas sumamente complejos, desarrollar teoría emergente y probar hipótesis, explorar y generalizar resultados, obteniendo la más amplia comprensión.

Fuente: Elaboración propia con información de (Hernández Sampieri & Mendoza Torres, 2018, pp. 631–649)

2.8 ANÁLISIS CRÍTICO DE LAS METODOLOGÍAS

Los tres enfoques, cuantitativo, cualitativo y mixto, son igualmente valiosos y son las mejores maneras existentes para investigar y generar conocimiento. La investigación, tal como menciona Sampieri (2014, p. 36) en términos generales, es un **conjunto de todos los procesos sistemáticos, críticos y empíricos** que se aplican al estudio de un ***fenómeno*** o ***problema***.

Hasta hace algún tiempo, los enfoques más conocidos eran el cualitativo y el cualitativo y eran vistos como "rivales" entre sí, pero hoy se consideran igual de importantes y necesarios, e

incluso, el campo de la investigación ha avanzado tanto que de alguna manera se ha logrado convertirlos en enfoques convergentes y complementarios, y es donde surge el enfoque mixto.

Ahondando un poco más en los enfoques cuantitativo y cualitativo, tal como lo menciona Sampieri (2018, p. 16) "la investigación cuantitativa ofrece la posibilidad de generalizar los resultados, otorga un punto de vista basado en conteos y magnitudes (…) por su parte, la investigación cualitativa proporciona profundidad a los datos, dispersión, riqueza interpretativa, contextualización del ambiente o entorno, detalles".

Aunque por si solos no son estos los seleccionados para el desarrollo de la investigación, a continuación, se presenta una tabla síntesis de las características principales de ambas metodologías, ver tabla 6.

Tabla 6. Comparativa elementos clave de las metodologías Cuantitativa y Cualitativa

Elemento o rubro de comparación	Ruta cuantitativa	Ruta cualitativa
Búsqueda de la objetividad	La objetividad es un estándar necesario (positivismo) o deseable (pospositivismo)	Admite subjetividad. Es parte del fenómeno y se analiza
Intenciones o metas de los estudios	Describir, explicar, comprobar o confirmar y predecir los fenómenos (establecer causalidad). Generar y probar teorías	Explorar, describir, comprender e interpretar los fenómenos, a través de las percepciones y significados producidos por las experiencias de los participantes. Generar teoría. Identificar conexiones entre componentes de los fenómenos (atribución de causalidad)
Tipo de datos	Numéricos (datos confiables y duros)	Narrativos (datos simbólicos y que generen significados y revelen experiencias, puntos de vista y cualidades)
Lógica del proceso (que guía la ruta)	Deductiva: de lo general a lo particular. En la ruta se transita de las leyes y la teoría a los datos y resultados	Inductiva: de lo particular a lo general. En la ruta se transita de los casos y datos a los resultados y la teoría
Diseño de la investigación	Estructurado, predeterminado e implementado según el plan (un mapa a seguir rigurosamente)	Abierto, flexible, construido durante el proceso. Es un abordaje que se adapta al contexto y las circunstancias

Elemento o rubro de comparación	Ruta cuantitativa	Ruta cualitativa
Muestra objetivo	Conjunto de casos que sea estadísticamente representativo de la población estudiada	Conjunto de casos que refleje las cualidades o atributos del fenómeno de interés o planteamiento del problema
Posición personal del investigador	Neutral e imparcial. El investigador trata de 'hacer a un lado' sus propios valores y creencias. Intenta asegurar procedimientos rigurosos y 'objetivos', así como evitar que sus sesgos y tendencias influyan en los resultados	Explícita. El investigador reconoce sus propios valores y creencias, incluso son fuentes de datos. Desde luego, pretende ser lo menos intrusivo posible en el estudio
Rol de la teoría y estudios previos	Crucial para afirmar el planteamiento del problema y guiar toda la investigación	Provee de dirección a la investigación junto con la evolución de los acontecimientos y desarrollo de la indagación
Papel de las hipótesis	Se establecen y prueban hipótesis. Se aceptan o rechazan dependiendo del grado de certeza (probabilidad)	Se generan hipótesis durante el estudio o al final de este. Las hipótesis son altamente contextuales (lugar y tiempo)
Instrumentos de recolección	Estandarizados. Su aplicación es uniforme en todos los casos.	Al inicio no se usan instrumentos completamente estandarizados, son flexibles y van afinándose conforme avanza el trabajo de recolección de los datos hasta alcanzar cierta homologación.
Finalidad de la recolección	Medir variables en casos.	Capturar significados, experiencias y reconstruir "realidades" de casos (individuos, grupos, comunidades y fenómenos).
Rol de los participantes	Fuentes externas de datos.	Fuentes internas de datos.
Propósito esencial del análisis	Describir las variables y sus relaciones, así como explicar los cambios. Establecer causalidad.	Describir experiencias, puntos de vista y hechos. Comprender personas, interacciones, procesos, eventos y fenómenos en sus contextos.
Criterios para evaluar la calidad	Objetividad, rigor, confiabilidad, validez, representatividad.	Credibilidad, confirmación, valoración, representatividad de voces y transferencia.

Elemento o rubro de comparación	Ruta cuantitativa	Ruta cualitativa
Presentación de Resultados	Estandarizado. Distribuciones de variables. Tablas, figuras y diagramas. Coeficientes estadísticos. Modelos estadísticos.	No estandarizado. Categorías, temas y patrones definidos y ejemplificados. Tablas, matrices y figuras que vinculan narrativas o categorías. Historias. Material simbólico: videos, fotografías, etc. Modelos conceptuales que representan experiencias, significados y construcciones de los participantes.

Fuente: Elaboración propia con información de (Hernández Sampieri & Mendoza Torres, 2018, pp. 12–14)

La selección de un enfoque mixto en la investigación se justifica por varias razones, principalmente debido a la naturaleza compleja de los fenómenos o problemas que acompañan esta investigación. Estos fenómenos están constituidos por dos realidades coexistentes: una **objetiva** y otra **subjetiva**, y para "***capturar***" ambas, se requieren tanto la visión objetiva como la subjetiva.

Principales razones por la que se seleccionó un enfoque mixto:

- Permite estudiar complejas realidades de comportamiento social.
- Se reconoce que ambos métodos son igualmente valiosos para el avance del conocimiento científico y que ninguno es intrínsecamente mejor que el otro.
- Ofrece una visión más integral, completa y holística del fenómeno estudiado.
- Caracterizan los objetos de estudio mediante números y lenguaje, recabando un amplio rango de evidencia.
- La triangulación (verificación de convergencia al contrastar datos de ambos enfoques), expansión (extensión del rango de indagación) y complementación (obtención de una visión más comprensiva) incrementan la validez interna y externa, y la confianza en que los resultados son una representación fiel del fenómeno.
- Permite explorar distintos niveles del problema y obtener una mayor variedad de perspectivas: frecuencia, amplitud y magnitud (cuantitativa), así como profundidad y complejidad (cualitativa).
- Reducción de incertidumbre.

- Los resultados de un método pueden informar al otro en cuestiones de muestreo, procedimientos, recolección y análisis de datos, incluso proveyendo de hipótesis y soporte empírico.

Seleccionar un enfoque mixto permite una comprensión más **integral y robusta** de los problemas de investigación complejos, aprovechando las fortalezas de los enfoques cuantitativo y cualitativo para obtener una visión holística y más profunda de la realidad.

2.9 HERRAMIENTAS PARA UTILIZAR

En la selección de las herramientas a utilizar en el desarrollo de la investigación intervienen varios factores que serán importantes también para el resto de la investigación, como ser el enfoque o metodología principal y sus objetivos.

La metodología define el tipo de herramienta que se utilizará, pues dependiendo de las características que se necesiten analizar se eligen las maneras de recolección de datos que permiten analizar y poder llegar a una conclusión.

2.9.1 GESTIÓN DE PROYECTOS

Para este trabajo de investigación se requiere una herramienta para organizar y dar seguimiento a todas las actividades del proyecto.

Contar con una herramienta de gestión de proyectos permite organizar y controlar de forma eficiente las tareas, plazos y recursos a utilizar, así como facilitar la comunicación y colaboración como equipo al centralizar la información en un solo espacio. En consecuencia, provee una visión clara del progreso, ayudando a identificar retrasos y asegurar el cumplimiento de los objetivos planteados.

- **JIRA**

Jira es una herramienta popular de gestión de proyectos que reúne amplias funciones para planificar, supervisar y entregar cualquier tipo de proyecto eficientemente.

Jira se adapta a cualquier proceso, técnica o metodología de gestión de proyectos, desde una planificación ágil hasta vistas perfectamente personalizables como listas de tareas, cronogramas, tableros Kanban y Scrum y más recientemente incorporando herramientas de inteligencia artificial para para impulsar la colaboración y mantener la coordinación más ágilmente.

El programa se puede conectar con aplicaciones como Microsoft Teams, pero se ve limitada en cuanto a la interconexión y funcionalidades con otras aplicaciones como Word, Outlook o el almacenamiento en la nube con OneDrive. De igual manera, la versión gratuita ofrece funcionalidades limitadas que impiden su utilización completa.

- **MICROSOFT PLANNER**

Microsoft Planner es una herramienta de gestión de proyectos nativa de Microsoft 365 que permite organizar el trabajo de forma visual y colaborativa.

Su estructura basada en tableros y columnas facilita la creación y asignación de tareas con fechas límite, con etiquetas y archivos adjuntos.

Es conveniente utilizarla por su capacidad de integración con aplicaciones como Microsoft Teams, Outlook y OneDrive, y, en este caso, cumple con el objetivo que se busca de coordinar equipos y dar seguimiento al progreso en tiempo real.

Tomando en cuenta las funcionalidades y ventajas que cada una de las aplicaciones mencionadas ofrece, se encuentra que **Microsoft Planner** es la opción más adecuada para el equipo de investigación, pues la institución educativa donde se cursa la maestría ofrece licencias de Microsoft 365 gratuita por su afiliación estudiantil, teniendo la posibilidad de utilizar todas las aplicaciones que esta suite ofrece y así sacarles el máximo provecho a los recursos ya disponibles.

Jira	Microsoft Planner
Conectividad limitada con aplicaciones de Microsoft.	Integración automática con otras aplicaciones de Microsoft 365.
Licencia necesaria para acceder a las funcionalidades clave.	Licencia necesaria para acceder a las funcionalidades principales. Adquirida por medio de licencia estudiantil.
Herramienta robusta con alta complejidad de configuración.	Interfaz visual estilo Kanban y configuraciones más sencillas para definir flujos de trabajo.
Enfocados en métricas de rendimiento, como ser tiempos de respuesta y finalización de asignaciones. Puede convertirse en una tarea complicada en caso de ser un proyecto a menor	Ofrece gráficos menos complejos, pero más fáciles de digerir por medio de la vista de un tablero Kanban y vista de calendario que integra Outlook.

escala.

2.9.2 RECOLECCIÓN DE DATOS

- **MICROSOFT FORMS**

Microsoft Forms es un programa para creación de formularios en línea, que tendrá como propósito el alojamiento del instrumento de recolección de datos, que, para conveniencia de los investigadores, permite crear enlaces para su envío masivo y las respuestas por parte de la muestra se pueden almacenar dentro de un archivo de Excel para su exportación.

Asimismo, Microsoft Forms también permite diferentes funcionalidades a la hora de construir la estructura de un formulario, como ser el *branching*, habilidad para redireccionar a otras preguntas en base a la respuesta de una persona, así como tener un límite de fecha y hora para poder llenar un formulario.

- **GOOGLE FORMS**

Google Forms es la solución que ofrece Google ante la necesidad de creación de formularios automatizados en línea. Se caracteriza por su curva de aprendizaje bastante corta y la opción de utilizar los gráficos que la aplicación genera automáticamente en base a las preguntas generadas, sin embargo, es limitado en cuanto a sus funciones de creación en sí; por ejemplo, solamente se puede limitar un formulario utilizando criterios como la cantidad de respuestas, pero no la duración de él.

Se debe tener en cuenta que la interconexión que esta aplicación posee se limita hacia los productos de Google, como ser Google Docs y Drive.

- **MICROSOFT EXCEL**

Microsoft Excel es un programa para crear y editar hojas de cálculo en donde es posible hacer limpieza de datos, cálculos estadísticos y creación de gráficos para sets de datos que no sean de gran escala, pues se tiene un límite de filas y columnas que la hoja de cálculo puede contener.

Excel, al utilizarse con la suite de Microsoft 365, permite conexiones con otras aplicaciones como Planner, Outlook y la nube de almacenamiento de OneDrive.

Para este caso, es una herramienta que ser plantea utilizar como intermediaria para conectar

los datos extraídos de encuestas y encuestas hacia una base de datos alojada en SQL, facilitando la integración de los datos a un sistema más potente y avanzado.

- **LIBREOFFICE CALC**

Calc, al igual que otros productos de LibreOffice mencionados anteriormente, representa una alternativa gratuita a Excel.

Este programa de hojas de cálculo ofrece funcionalidades similares a Excel, con la diferencia que no es posible conectarse con aplicaciones que pertenezcan a la suite de Microsoft 365, así como limitaciones para conectar el programa a un motor de base de datos.

Tomando en cuenta las funcionalidades que cada programa ofrece, se encuentra que **Microsoft Forms y Microsoft Excel** son las herramientas más idóneas para poder realizar los trabajos de recolección y limpieza de datos, pues el solo hecho de contar con la integración de Microsoft 365 facilita el flujo de trabajo al evitar la etapa de procesamiento de respuestas y transferencia de datos hacia otro software, teniendo todo en un lugar centralizado; de igual manera, la institución educativa donde se cursa la maestría ofrece licencias de Microsoft 365 gratuita por su afiliación estudiantil, teniendo la posibilidad de utilizar todas las aplicaciones que esta suite ofrece y así sacarles el máximo provecho a los recursos ya disponibles.

Microsoft Forms	**Google Forms**
Integración automática con otras aplicaciones de Microsoft 365.	Integración automática con suite de Google (Docs, Drive).
Licencia necesaria para acceder a las funcionalidades principales.	Software de acceso libre y gratis.
Configuraciones específicas de formularios (Branching, límite de fecha y hora para responder)	Limitaciones para la configuración de formularios. (Branching no permite condiciones complejas, diseño para cerrar formularios depende de ser manual o por límite de respuestas)

Microsoft Excel	**LibreOffice Calc**
Integración automática con otras aplicaciones	Falta de conectividad con otras aplicaciones del

de Microsoft 365.	ecosistema LibreOffice.
Licencia necesaria para acceder a las funcionalidades principales.	Software de acceso libre y gratis.
Posee diferentes herramientas automatizadas y semiautomatizadas para la preparación, modelado y transformación de datos.	Funciones limitadas para la preparación, modelado y transformación de datos, siendo herramientas y fórmulas manuales las que se proveen.

2.9.3 ANÁLISIS DE DATOS

- **SQL**

SQL, o *Structured Query Language* por sus siglas en inglés, es un lenguaje para el procesamiento, visualización y manipulación de datos. Comúnmente se utiliza en diferentes motores de base de datos, para lo cual se alojan los datos en tablas y el lenguaje asiste y proporciona una manera de visualizarlos en reportes.

El propósito de utilizarlo en esta investigación es para poder procesar los reportes obtenidos de atención y soporte al usuario final obtenidos de la plataforma de atención al usuario que la organización tiene, de esta manera calculando lo necesario para tener las métricas MTTD y MTTR.

Existen diferentes motores de base de datos, como ser **PostgreSQL, Microsoft SQL Server y Oracle Database Engine.**

- **PostgreSQL** es un motor de base de datos de código abierto y gratis, el cual posee diferentes herramientas y características que permiten expandir dentro de las habilidades que trae por defecto.

  Es posible conectar el motor con sistemas de procesamiento geográfico, así como expandir procedimientos almacenados utilizando otros lenguajes aparte de SQL, como ser Python o Javascript y tiene soporte nativo para manejar objetos de tipo JSON, permitiendo la combinación e integración de diferentes fuentes de datos en un solo lugar.

  Normalmente, se utiliza en proyectos de desarrollo de aplicaciones web y modelado de datos complejos.

- **SQL Server,** cuya última versión comercial es del año 2022, es el motor de base de datos de Microsoft, el cual permite escalabilidad comercial y módulos de analítica.

  La licencia necesaria para operar SQL Server tiene un precio bastante alto y está orientado hacia la utilización de este en entornos empresariales; incluyendo características de analítica y su fácil integración con otros programas de Microsoft, suele ser una solución atractiva para empresas que buscan la inteligencia empresarial.

  Para el caso del uso estudiantil y contextos de investigación, existe la versión Express, cuya limitación principal es el espacio de 2 GB permitidos, dentro de los cuales no se espera que se aloje una aplicación robusta o datasets extensivos.

- **Oracle Database Engine** es un motor de base de datos con modelo de pago de licencia, diseñado para trabajar con cargas de datos masivas y la creación de data warehouses.

  Es utilizado con mayor provecho al integrar otras aplicaciones de Oracle, como ser Oracle APEX y cuenta con tecnologías que permiten alta disponibilidad y optimización del motor a nivel de hardware, como el manejo de memoria dinámica y planes de optimización automáticos. Su alto nivel de complejidad para manejar es algo que se debe tener en cuenta para proyectos a menor escala.

- **KNIME**

Knime es un programa para procesamiento estadístico de datos, el cual funciona como un creador de flujos que se pueden automatizar para obtener métricas y elementos estadísticos. Permite integrar diferentes fuentes de datos y su curva de aprendizaje es menor para personas que no tienen experiencia con herramientas tecnológicas o de informática.

Knime es de uso libre y gratuito, con herramientas y complementos creados en diferentes lenguajes de programación por una comunidad que permiten expandir el uso de este.

Para el propósito de la investigación, se utilizará para obtener promedios, varianzas e

histogramas que analizarán los datos del MTTR y de esta manera, poder generar análisis que se agregarán a la triangulación de datos.

- **SPSS**

SPSS es un programa de IBM orientado al análisis de datos y aplicaciones estadísticas para el área de estudios sociales, así como el área matemáticas y academia en general.

Su interfaz es fácil de utilizar para personas no familiarizadas en el campo del análisis y permite hacer cálculos complejos con sets de datos robustos.

Permite la integración con datos provenientes de archivos planos (como ser CSV) y de motores de bases de datos por medio de conexiones ODBC, sin embargo, no tiene soporte para fuentes de datos más modernas como archivos JSON o conexión a APIs.

SPSS se vale por una licencia, la cual es inaccesible para usuarios que planean utilizarlo para proyectos de menor escala, mientras que la versión de prueba es de tiempo limitado y sus funcionalidades se encuentran inaccesibles o limitadas de alguna manera.

Knime	SPSS
No tiene costo, es licencia de uso libre.	Licencias con alto nivel monetario y su versión de prueba está limitada en tiempo y funcionalidad.
Permite integrar diferentes fuentes de datos modernas como APIs y sus funcionalidades se pueden expandir por medio del uso de herramientas como Python o R.	La integración de fuentes de datos es limitada, solamente hacia archivos planos (CSV), motores de base de datos y otros archivos de SPSS. No permite ingresar lenguajes de programación para expandir funcionalidades,
Flujos de trabajo visuales y detallados que muestran el proceso de transformación y procesamiento de manera clara y ordenada.	Dificultad para mostrar los pasos del análisis pues todo se desarrolla en la misma pantalla sin dejar registro o bitácora de los pasos tomados para realizar el análisis.

2.9.4 GESTIÓN DE REFERENCIAS

Para gestionar de mejor manera nuestras fuentes bibliográficas surge la necesidad de contar con una herramienta informática diseñada para organizar, almacenar y dar formato a las fuentes bibliográficas utilizadas en nuestro trabajo de investigación, y que facilite la inserción de citas de forma automática en el texto y a generar bibliografías con el estilo APA requerido.

- **ZOTERO**

En el caso de la investigación, la herramienta seleccionada es Zotero, un software gratuito y de código abierto especializado en la gestión de referencias, permite guardar automáticamente fuentes desde navegadores, organizarlas y añadir notas o etiquetas personalizadas. Se integra automáticamente con herramientas de ofimática como Microsoft Word para insertar citas y bibliografías de manera sencilla.

2.10 MARCO LEGAL

Legislación Centroamericana sobre la Gestión de Riesgos de TI

Guatemala

Publicada el 1 de diciembre de 2021 en su diario oficial "Diario de Centro América" presenta la resolución JM-104-2021 de la Junta Monetaria de Guatemala, mediante la cual se aprueba el Reglamento para la Administración del Riesgo Tecnológico. Esta tiene como objetivo establecer los lineamientos mínimos que los bancos, las sociedades financieras, las entidades fuera de plaza o entidades off shore y las empresas especializadas en servicios financieros que forman parte de un grupo financiero. Este documento representa un parteaguas para el resto de las instituciones guatemaltecas que pueden adoptarlo como ejemplo, y que, en su forma más integral, este se compone de definiciones y regulaciones sobre tópicos como la administración del riesgo tecnológico, infraestructura de TI, sistemas de información, bases de datos y servicios de TI, seguridad de tecnología de la información, ciberseguridad, plan de recuperación de desastres y procesamiento y/o almacenamiento de información. (JUNTA MONETARIA, BANCO DE GUATEMALA, 2021)

El Salvador

El poder legislativo salvadoreño emite el 15 de noviembre de 2024, bajo el tomo 445, número 219 (2024, pp. 3–22), la Ley de Ciberseguridad y Seguridad de la

Información, estableciendo así un marco normativo para estructurar, regular, auditar y fiscalizar las medidas de ciberseguridad y seguridad de la información en las instituciones públicas.

Nicaragua

Nicaragua lleva la delantera y lidera la gestión de los riesgos de TI, desde el año 2007 emitió la Norma sobre gestión de riesgo tecnológico, cuyo objetivo es establecer los criterios mínimos de evaluación sobre la administración de los riesgos, la seguridad, la utilización y los controles aplicados a las TIC, con el fin de velar por la estabilidad y la eficiencia del sistema financiero. Al igual que en el caso de Guatemala, el alcance de esta normal es aplicable a instituciones financieras, pero perfectamente pueden tomarse como base para la gestión del riesgo en el sector privado. (SUPERINTENDENCIA DE BANCOS Y DE OTRAS INSTITUCIONES FINANCIERAS, 2007, p. 7077)

Costa Rica

Actualiza en el 2021 las Normas técnicas para la gestión y el control de las Tecnologías de Información, sustituyendo su versión predecesora (N-2-2007-CODFOE) derogadas por la Contraloría General de la República mediante la resolución N° R-DC-17-2020 del diecisiete de marzo del dos mil veinte. En ella tipifica la regulación e importancia de contar con "un proceso formal de gestión de riesgos que responda a las amenazas que puedan afectar el logro de los objetivos institucionales, basado en una gestión continua de riesgos que este integrada al sistema especifico de valoración del riesgo institucional" (Solís García et al., 2021, p. 11)

Panamá

Con la legislación gubernamental más completa de la región, redacta en 2017 un documento de más de 70 páginas que comprende normas y leyes, estructura de TI, procedimientos, pautas para mantenimientos de sistemas, continuidad del servicio, monitoreo, bitácoras, seguridad informática, uso y manejo de la información, temas en control de accesos, correcto uso de internet y la nube, hosting y por supuesto la administración integral del riesgo, entre otros tópicos de gran impacto en TI. Establece que "Se debe realizar una evaluación del riesgo, con base a la metodología adoptada, por lo

menos una vez al año y el informe de resultados debe ser presentado a la máxima autoridad de la Entidad."(Dirección Nacional de Gobernanza de TI, 2017, p. 44)

Honduras

En Honduras, no existe una legislación específica sobre gestión de riesgos de TI, sino que se aplican normativas sectoriales como la presentada por la Comisión Nacional de Bancos y Seguros (CNBS), que al igual que las regulaciones de Guatemala y El Salvador está específicamente dirigidas al sector bancario. También existe la Ley del Sistema Nacional de Gestión de Riesgos (SINAGER) del 2009 establece el marco para la gestión integral de riesgos, que puede ser aplicable a riesgos de TI, pero sin tratar el tema en específico.

Centrándose en el primer documento mencionado, la CNBS (2022) establece regulaciones del tipo

Artículo 4.- Gestión de los riesgos asociados con tecnologías de información:

"Las Instituciones Supervisadas deben garantizar que su Marco de Gobierno de Riesgo contemplen lo relacionado con las TI como un proceso institucional, transversal, coherente con los objetivos estratégicos y el plan de negocios…"

Artículo 5.- Gobierno de TI:

"Gestión de Riesgos Asociados con TI: Identificar, evaluar, mitigar, monitorear y comunicar los riesgos asociados con TI, alineado al Marco de Gobierno de Riesgo definido por la Institución Supervisada."

Artículo 7.- Gestión de TI:

"Las Instituciones Supervisadas deben diseñar, implementar, documentar, monitorear y actualizar el Marco de Gestión de TI…"

Artículo 8.- Organización del área de TI:

"El área de TI debe gestionar los riesgos materiales a las tecnologías de la información como primera línea de defensa…"

Artículo 17.- Gobierno de seguridad de la información y ciberseguridad:

"Gestión de los Riesgos: Administrar efectivamente los riesgos de seguridad de la información y ciberseguridad, para mitigar o reducir su impacto de acuerdo con el apetito y tolerancia al riesgo definido."

Artículo 18.- Marco de gestión de seguridad de la información y ciberseguridad

"La implementación de una metodología de gestión de riesgos de seguridad de la información y ciberseguridad alineada con el Marco de Gobierno de Riesgo de la Institución."

Artículo 19.- Gestión de la ciberseguridad:

"Las Instituciones Supervisadas deben gestionar la ciberseguridad basado en las mejores prácticas y estándares internacionales que les permita: Identificar, Proteger, Detectar, Responder, Recuperar y Aprender."

Artículo 28.- Evaluación y análisis de riesgos:

"Las Instituciones Supervisadas deben identificar y evaluar los riesgos que podrían causar una interrupción del negocio, aplicando una metodología consistente con la utilizada para la evaluación de los riesgos operativos."

Artículo 40.- Auditoría basada en riesgos:

"La planificación de auditoría de sistemas, de conformidad con la metodología de auditoría, debe ser con base en los riesgos asociados a las TI…"

Artículo 42.- Resguardo y monitoreo de bitácoras:

"Las Instituciones Supervisadas deben resguardar las bitácoras de auditorías de los sistemas… y deben ser monitoreados por las funciones de vigilancia correspondientes.

Lo anterior, si bien demuestra un avance nacional en la regulación de la gestión de riesgos de la seguridad de la información como parte del área de TI, al menos por ahora en el sector bancario, también revela que queda mucho camino por recorrer para contar con una regulación integral que comprenda al menos todas las instituciones públicas y que pueda servir de base para la adopción de normativas de la misma índole en el sector privado.

CAPÍTULO III. METODOLOGÍA

3.1 CONGRUENCIA METODOLÓGICA

3.1.1 MATRIZ METODOLÓGICA

Nombre de la Investigación	Problema	Pregunta(s) de Investigación (PICO)	Objetivos de la Investigación (SMART)	Metodología	Instrumentos	Variables	Indicadores
Brecha de Conocimiento en la Gestión de Riesgos de TI en el Sector Farmacéutico Hondureño: Estudio de Caso en Distribuidora Leterago y Laboratorio Megalabs 2025	La falta de un modelo formal de gestión de riesgos de TI genera vulnerabilidades, tiempos de respuesta prolongados y una asignación ineficiente de recursos, debilitando la resiliencia institucional.	**Pregunta General:** ¿Cómo la (I) brecha de conocimiento existente en gestión de riesgos de la seguridad de la información en (P) el área de TI de Distribuidora Leterago, en (C) comparación con las mejores prácticas definidas en el marco normativo ISO 27005, (O) impacta en la exposición a vulnerabilidades y la eficiencia en la respuesta a incidentes?	**Objetivo General:** Diagnosticar la brecha de conocimiento en la gestión de riesgos de la seguridad de la información dentro del área de TI de Distribuidora Leterago para determinar su impacto en la exposición a vulnerabilidades y la eficiencia operativa, (M) mediante encuestas y análisis documental de reportes de incidentes, (R) para generar un diagnóstico base que informe futuras estrategias de mitigación, (T) durante el último trimestre de 2025.	Enfoque: Mixto. Diseño: Exploratorio Secuencial (DEXPLOS). Diseño: Transversal (2025) Tipo de Estudio: Estudio de Caso Único. Estrategia: Triangulación de datos (metodológica, de datos y teórica).	Encuesta (Microsoft Forms) Extracción de datos históricos (Base de datos Sistema de Tickets para MTTD/MTTR). **Escala de Likert para datos cuantitativos** Análisis documental (Políticas, manuales). Encuesta (Microsoft Forms) **Para datos cualitativos**	**Variables Independientes:** Brecha de Conocimiento (Dimensión 1: Conocimiento; Dimensión 2: Aplicación de prácticas). **Variables Dependientes:**	Nivel de competencia (Escala 1-5) por dominio de ISO 27005. Resultados de la encuesta y matriz de evaluación.

Nombre de la Investigación	Problema	Pregunta(s) de Investigación (PICO)	Objetivos de la Investigación (SMART)	Metodología	Instrumentos	Variables	Indicadores
		Preguntas Específicas:	**Objetivos Específicos:**			1. Exposición a Vulnerabilidades.	- Número de incidentes de seguridad reportados en el último año, clasificados por criticidad (Alto, Medio, Bajo).
		¿De qué manera el (I) nivel de conocimiento y aplicación de las prácticas actuales de gestión de riesgos que ejecuta (P) el personal de TI de Distribuidora Leterago, en (C) comparación con los dominios de competencia definidos en ISO 27005, (O) evidencia la magnitud de la brecha de conocimiento existente?	Determinar el nivel de conocimiento sobre gestión de riesgos de la seguridad de la información en el personal de TI, (M) utilizando una matriz de competencias basada en ISO 27005 y (A) encuestas a todo el personal del área, (R) para cuantificar la brecha de habilidades, (T) en un plazo de cinco semanas.			2. Eficiencia Operativa	Tiempo Medio de Detección (MTTD) en horas. Tiempo Medio de Respuesta (MTTR) en horas.

Nombre de la Investigación	Problema	Pregunta(s) de Investigación (PICO)	Objetivos de la Investigación (SMART)	Metodología	Instrumentos	Variables	Indicadores
		En (P) la estructura y cultura de Distribuidora Leterago, ¿de qué manera los (I) factores organizacionales, como la falta de políticas formales, en (C) comparación con organizaciones con una cultura de seguridad madura, (O) contribuyen a perpetuar la brecha de conocimiento en gestión de riesgos?	Identificar los factores organizacionales que perpetúan la brecha de conocimiento, (M) mediante el análisis de la documentación de políticas y (A) encuestas con los líderes de equipo, (R) para comprender las causas raíz culturales, (T) en un plazo de seis semanas.				
		¿En qué medida los valores de indicadores operativos como el Tiempo Medio de Detección y el Tiempo Medio de Respuesta (I) sirven como indicadores efectivos del nivel de eficiencia operativa (O) del área de TI de	Determinar el nivel de eficiencia operativa por medio de la respuesta a incidentes, (M) analizando el Tiempo Medio de Detección (MTTD) y Respuesta (MTTR) de los (A) incidentes reportados en los últimos 12 meses, (R) para conectar			**Variables Mediadoras:** Factores Organizacionales (Cultura, Políticas, Apoyo).	Presencia/Ausencia de cultura de mejora continua. Número de políticas documentadas (ej. 0-5). Frecuencia de declaraciones de apoyo y asignación de recursos por parte de la dirección.

Nombre de la Investigación	Problema	Pregunta(s) de Investigación (PICO)	Objetivos de la Investigación (SMART)	Metodología	Instrumentos	Variables	Indicadores
		Distribuidora Leterago (P) en comparación con organizaciones que tienen una cultura de seguridad madura (C), según un análisis de los datos obtenidos en los últimos 12 meses (T)?	la brecha de conocimiento con resultados operativos, (T) en un plazo de ocho semanas.				

3.1.2 ESQUEMA DE VARIABLES DE ESTUDIO

La investigación en curso consiste en diagnosticar la brecha de conocimiento en la gestión de riesgos de seguridad de la información y su impacto en la exposición a vulnerabilidades y la eficiencia operativa. Esta brecha actuará como la **variable independiente (VI)** compuesta por dos dimensiones principales, que son el *conocimiento sobre la gestión de riesgos de seguridad de la información* y la *aplicación de prácticas*. Su impacto se mide a través de dos **variables dependientes (VD)**, exposición a vulnerabilidades y la eficiencia operativa. Además, se identifican factores organizacionales que actúan como **variables mediadoras (VM),** ya que explican e intervienen en la relación entre brecha de conocimiento persiste y cómo afecta a las variables dependientes, ver figura 3.

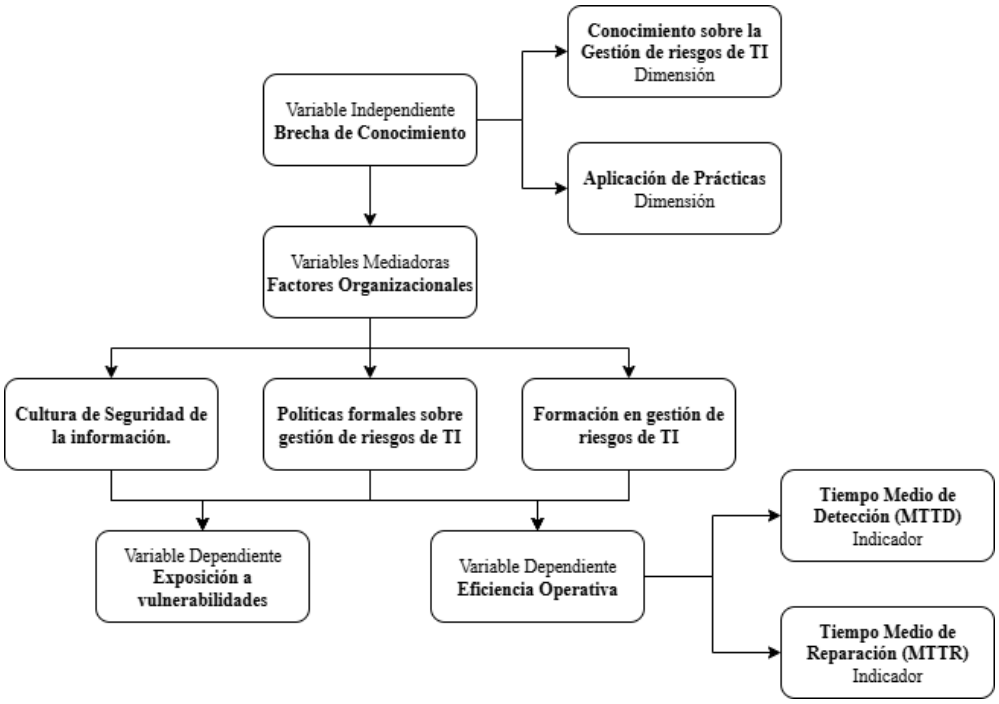


Figura 3. Esquema de Variables de Estudio

Fuente: Elaboración propia

3.1.3 OPERACIONALIZACIÓN DE VARIABLES

A continuación, se presenta la operacionalización de las variables clave enumeradas en la sección anterior, se resume en la tabla 5. Este paso convierte las variables de conceptos meramente abstractos en elementos **medibles.**

Tabla 5. Operacionalización de variables

Variable Conceptual	Dimensión	Definición Operacional	Indicador
1. Brecha de Conocimiento (VI)	Conocimiento sobre la Gestión de riesgos de seguridad de la información	Grado de familiaridad y comprensión del personal de TI sobre los principios, marcos de trabajo y mejores prácticas de TI y procesos de gestión de riesgos de seguridad de la información.	Escala: Nivel de competencia (Ej.: 1-5) por dominio. Análisis de Encuestas a todo el personal seleccionado en la muestra.
	Aplicación de Prácticas	Grado en el que el personal aplica efectivamente las prácticas de gestión de riesgos en sus actividades diarias y en la respuesta a incidentes.	

Variable Conceptual	Dimensión	Definición Operacional	Indicador
2. Factores Organizacionales (VM)	Cultura de Seguridad de la información.	Valores, actitudes y comportamientos compartidos dentro de la organización respecto a la importancia de la seguridad de la información y la gestión de riesgos.	Indicador: Presencia/ausencia de una cultura de mejora continua y aprendizaje frente a incidentes.
	Políticas formales sobre gestión de riesgos de seguridad de la información	Existencia, claridad y formalización de políticas, procedimientos y marcos de trabajo escritos para la gestión de riesgos.	Indicador: Número de políticas documentadas (ej.: 0-5).
	Formación en gestión de riesgos de TI	Grado de compromiso, apoyo en la capacitación de la gestión de riesgos por parte de la alta dirección y los mandos medios.	Indicador: Frecuencia de declaraciones de apoyo y asignación de recursos.
3. Exposición a Vulnerabilidades (VD)	Nivel de Riesgo	Grado de susceptibilidad de los activos de TI a amenazas, explotación o compromiso debido a controles insuficientes.	Indicador: Número de incidentes de seguridad reportados en el año en curso, clasificados por criticidad (Alto, Medio, Bajo).
4. Eficiencia Operativa (VD)	Velocidad de Respuesta	Capacidad del área de TI para contener, erradicar y recuperarse de un incidente de seguridad.	Indicador: Tiempo Medio de Respuesta (MTTR) en horas.

Fuente: Elaboración propia

3.1.4 HIPÓTESIS

Según el carácter exploratorio de nuestra investigación se han definido dos conjuntos de hipótesis.

1) Hipótesis para la Relación entre el departamento del empleado y su nivel de capacitación recibida en ciberseguridad.

   a. H_0 (Hipótesis Nula): *No existe diferencia significativa en el nivel de capacitación en ciberseguridad recibido por los empleados de diferentes departamentos de la empresa.*

   b. **Hipótesis Alternativa (H_1):** *Existe una diferencia significativa en el nivel de capacitación en ciberseguridad recibido por los empleados según el departamento al que pertenecen.*

2) Hipótesis para la Variable Dependiente: **Eficiencia Operativa**

   a. **Hipótesis Nula (H_0):** *No existe una relación significativa entre la brecha de*

conocimiento en gestión de riesgos de seguridad de la información, el departamento en que se labora y su importancia en la eficiencia operativa para los empleados administrativos en Distribuidora Leterago.

b. **Hipótesis Alternativa (H_1):** *Existe una relación significativa entre la brecha de conocimiento en gestión de riesgos de seguridad de la información, el departamento en que se labora y su importancia en la eficiencia operativa para los empleados administrativos en Distribuidora Leterago. A mayor brecha de conocimiento, menor importancia con la eficiencia operativa.*

3.2 ENFOQUE O TIPO DE INVESTIGACIÓN

La investigación adoptará un enfoque mixto, con un diseño exploratorio secuencial (DEXPLOS - fase cualitativa seguida de fase cuantitativa) seleccionada para diagnosticar la brecha de conocimiento en la gestión de riesgos de riesgos de seguridad de la información en la filial Honduras de Distribuidora Leterago y Laboratorios Megalabs.

El fenómeno bajo estudio presenta dos dimensiones simultáneas, por un lado, se tiene una dimensión objetiva y medible (métricas como **MTTR**, además de **cantidad y nive**l de riesgo de vulnerabilidades, etc.) y por el otro, una dimensión subjetiva y más interpretativa (como **conocimientos o brechas de conocimiento**, percepciones, cultura organizacional, prácticas o métodos informales, etc.).

Para capturar ambas dimensiones de forma rigurosa se adoptará una postura epistemológica pragmática que permite combinar métodos positivistas (**cuantitativos**) para medir y generalizar efectos operativos, con enfoques interpretativos (**cualitativos**) que exploran causas, significados y barreras culturales. Tal como lo define Sampieri & Mendoza Torres (2018, p. 663):

> "El sustento filosófico de los métodos mixtos es el **pragmatismo**, el cual sugiere usar el método más apropiado para un estudio específico, y constituye una orientación filosófica y metodológica"

Ontológicamente, esta postura asume una realidad plural: existen hechos observables y medibles y realidades construidas socialmente como percepciones, ambos igualmente relevantes para comprender cómo la brecha de conocimiento impacta la exposición a vulnerabilidades y la eficiencia de respuesta.

Metodológicamente el enfoque mixto parece ser la mejor opción, dado que este facilita la triangulación de evidencia (**percepciones vs. evidencia documental y métricas**) y aumenta la credibilidad de las inferencias. (Hernández Sampieri et al., 2014).

3.3 ALCANCE

El alcance de esta investigación se ha definido como **exploratorio**, considerando que la tarea de analizar la brecha de conocimiento dentro del sector farmacéutico no se ha discutido en literaturas e investigaciones pasadas. La problemática que se define a raíz del desarrollo de la investigación con su alcance debe arribar hacia la creación de objetivos que también reflejen este hilo conductor.

Hernández Sampieri & Mendoza Torres, (2018) definen este desarrollo de una investigación como el que se lleva a cabo cuando se necesita tomar un fenómeno del que no existan registros anteriormente, proponiendo que en caso de que el tema principal de la investigación se busque en literaturas e investigaciones del pasado y no se encuentren símiles, lo más apropiado es dirigirlo hacia este enfoque.

Por lo tanto, los investigadores consideran que, al ser un fenómeno del cual no se han delimitado y observado sus características, tampoco es posible crear una hipótesis en base a lo recolectado en las etapas anteriores de la investigación y, para sintetizar lo planteado por (Ramos Galarza, 2020), por la propia naturaleza de la investigación exploratoria no es posible la realización de proyecciones o predicciones acerca de un fenómeno si no se tiene la información suficiente.

La construcción de características generales en base a las interacciones que el ser humano tiene con este fenómeno es necesaria para sentar una base metodológica y medible que permita "(…) recabar información que permita, como resultado del estudio, la formulación de una hipótesis". (Arias, 2012)

3.4 DISEÑO DE LA INVESTIGACIÓN

Se seleccionó un diseño **transversal** por la naturaleza del fenómeno que busca explorar la brecha de conocimiento en la gestión de riesgos de la seguridad de la información en un momento específico del tiempo, identificando categorías y relaciones relevantes a partir de información cualitativa para luego medirlas cuantitativamente. Este diseño es idóneo para fenómenos como el presente que son poco o nulamente estudiados o con instrumentos no validados, y permite generar

conocimiento preliminar y construir bases para posteriores análisis correlacionales o causales.

El diseño transversal facilita la integración y triangulación de métodos cualitativos y cuantitativos dentro de un mismo periodo temporal, optimizando recursos y garantizando la coherencia con el enfoque mixto adoptado (Hernández Sampieri & Mendoza Torres, 2018).

3.4.1 POBLACIÓN

La población **finita** seleccionada para la investigación es **la totalidad de los empleados** que pertenecen a Distribuidora Leterago y la compañía que está ligada a ellos, Laboratorios Megalabs, en la **sucursal de Honduras**, de la cual existen registros documentales que gestiona el área de Recursos Humanos, en este caso llamada *Personas y Cultura*, el cual almacena registro de los empleados activos de toda la empresa y, dentro de lo que la investigación concierne, solo se utilizará la cantidad de empleados asignados a las diferentes áreas que existen en la sucursal de Honduras, como ser:

- **Administración y Finanzas**
- **Comercial**
- **Operaciones**
- **Personas y Cultura**
- **Regencia y Calidad**
- **Tecnología Informática**

Para diferenciar la delimitación de una población contra la de un *universo*, es necesario plantear que un universo como tal comprendería un conjunto más amplio y generalizado de elementos o personas, como ser “todos los empleados del sector farmacéutico en Honduras”. Al definir la población dentro de la totalidad de los empleados que pertenecen a Distribuidora Leterago y Laboratorios Megalabs, se están tomando empleados que comparten características clave que permiten la formulación de los pasos para la creación de instrumentos de recolección, así como las conclusiones de la investigación como tal, todo esto siendo delimitado por el problema inicial y los objetivos de estudio, como lo plantea (Arias, 2012).

Al momento de la investigación, la totalidad de empleados que pertenecen a Distribuidora Leterago y Laboratorios Megalabs es de **132 empleados activos**. Ver tabla 7.

Tabla 7: Muestra de la tabla de Excel donde se consolida la población en base a fuentes secundarias

ID Poblacion	Area o Puesto	Empresa Perteneciente	Tipo de Empleado
1	ADMINISTRACIÓN Y FINANZAS	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
2	ADMINISTRACIÓN Y FINANZAS	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
3	ADMINISTRACIÓN Y FINANZAS	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
4	ADMINISTRACIÓN Y FINANZAS	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
5	ADMINISTRACIÓN Y FINANZAS	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
6	ADMINISTRACIÓN Y FINANZAS	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
7	ADMINISTRACIÓN Y FINANZAS	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
8	ADMINISTRACIÓN Y FINANZAS	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
9	ADMINISTRACIÓN Y FINANZAS	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
10	ADMINISTRACIÓN Y FINANZAS	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
11	ADMINISTRACIÓN Y FINANZAS	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
12	ADMINISTRACIÓN Y FINANZAS	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
13	ADMINISTRACIÓN Y FINANZAS	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
14	COMERCIAL	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
15	COMERCIAL	DISTRIBUIDORA LETERAGO	OPERATIVO
16	COMERCIAL	DISTRIBUIDORA LETERAGO	OPERATIVO
17	COMERCIAL	DISTRIBUIDORA LETERAGO	OPERATIVO
18	COMERCIAL	DISTRIBUIDORA LETERAGO	OPERATIVO
19	COMERCIAL	DISTRIBUIDORA LETERAGO	OPERATIVO
20	COMERCIAL	DISTRIBUIDORA LETERAGO	OPERATIVO

Fuente: Elaboración propia

3.4.2 MUESTRA

Para el caso de esta investigación la selección de la **muestra** se orientará a un tipo de muestreo **no probabilístico**, el cual se caracteriza por la selección de la muestra orientada a la identificación de características comunes entre la población total. (Arias González & Covinos Gallardo, 2021)

Distribuidora Leterago y Laboratorios Megalabs hacen la distinción dentro de su estructura organizacional los puestos y plazas que se consideran **Administrativos** u **Operativos**, para lo que se toman criterios como el área de trabajo, sus funciones asignadas y habilidades requeridas para desarrollarse.

Existen 90 personas que se consideran Operativas y 42 personas que se consideran Administrativas, como se puede ver en la siguiente gráfica, ver figura 4:

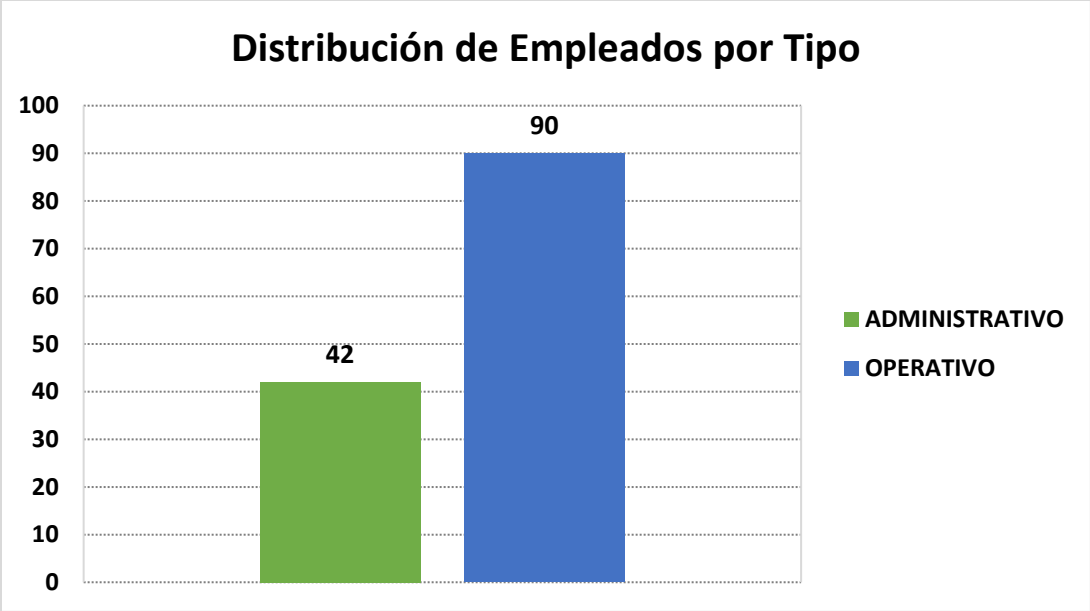


Figura 4. Categorización de empleado por la naturaleza de su posición laboral en Distribuidora Leterago y Megalabs.

Fuente: Elaboración propia.

La muestra se delimitará a la cantidad de personas que dentro de la gestión de personal de la empresa se denominan como **"Administrativos"**, de los cuales en la sucursal de Honduras de la Distribuidora Leterago y Laboratorios Megalabs, se encuentran **42 personas**, de esta manera utilizando el criterio de utilizar una misma característica que comparten, sin embargo, debe tenerse en cuenta que no se debe incluir a una de las personas que realiza esta investigación y actualmente labora en Distribuidora Leterago, por lo que la muestra se compondrá de **41 personas.**

Se considera que estas personas conciernen de más interés a los investigadores, pues por las habilidades requeridas para ejercer en estos puestos, la empresa les asigna equipo tecnológico como ser computadoras portátiles o de escritorio, así como concederle acceso al vasto entorno tecnológico, dentro de lo que comprende acceso a la nube de OneDrive para almacenar documentos y/o acceso a las diferentes carpetas compartidas que pertenecen al área asignada. En cambio, el personal **operativo** es asignado con dispositivos móviles cuyo entorno tecnológico es limitado al acceso de documentos pertinentes a las funciones que desarrollan en su campo de trabajo.

3.4.3 TÉCNICAS DE MUESTREO

Para efectos de esta investigación y por los motivos orientados a preservar el criterio por

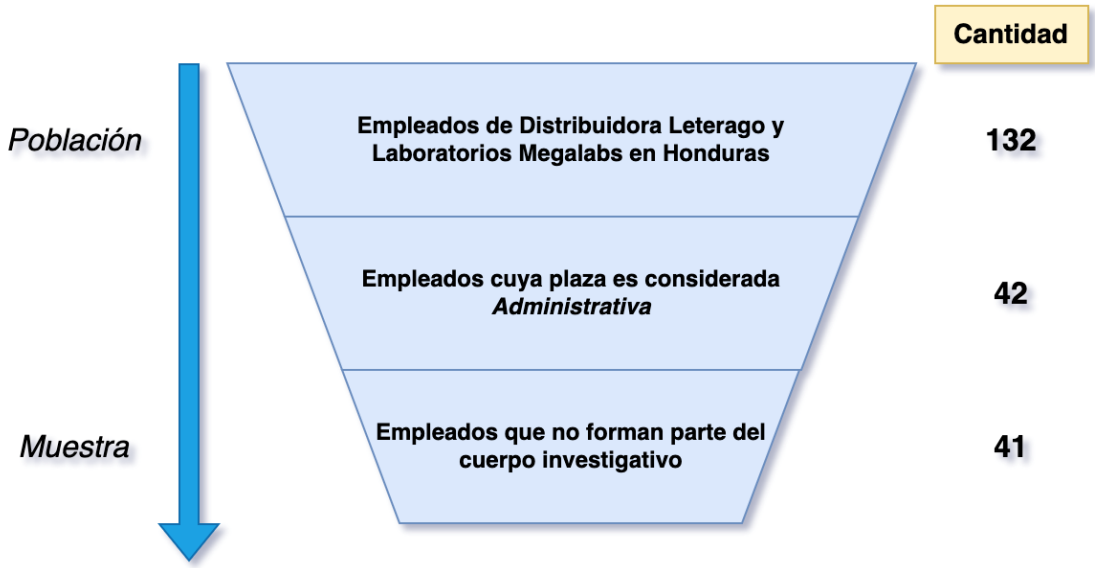
medio de varias características, se utilizará el **muestreo por cuotas**, el cual se define como "la elección de los elementos en función de ciertas características de la población, de modo tal que se conformen grupos o cuotas correspondientes con cada característica" (Arias, 2012).

El razonamiento principal es que, por interés de los investigadores, se seleccionarán para el llenado de la encuesta usuarios finales que dentro del organigrama general entran en puestos **Administrativos** y no están involucrados de manera activa en la investigación, significando que no forman parte de la creación del documento.

Para realizar el muestreo por cuotas, primero es necesario delimitar la distribución de plazas que hay que dentro de toda la sucursal de Honduras de la Distribuidora Leterago, y al hacerlo, se está encontrando qué proporciones existen sobre cada uno de los puestos, proceso que se detallará dentro del criterio de selección de la muestra.

3.4.4 CRITERIO DE SELECCIÓN DE LA MUESTRA

Para definir correctamente criterios de selección y exclusión que se les aplicará a los integrantes de la muestra, es necesario tener la habilidad de sintetizar y resumir información para formar una vista integral del aspecto evaluado. Ver figura 5.



.

Figura 5. Esquema de Funnel para la se elección de la muestra

Fuente: Elaboración propia

Por el motivo de limitantes con el tiempo de estudio para la investigación, así como la disposición a mano de recursos de los investigadores, se priorizó utilizar la sucursal de Honduras

de la Distribuidora Leterago, y en específico, las personas con puestos **Administrativos**, lo cual significa que estas personas **forman parte activamente** en los procesos administrativos de la empresa, utilizan equipo informático de la empresa como ser computadoras portátiles o de escritorio, en donde tienen acceso al entorno tecnológico (que incluye acceso al almacenamiento de nube, carpetas compartidas alojadas en el servidor propio de la empresa y al ERP, por lo cual la gestión de riesgos orientada a las funciones de estas personas aumenta un nivel de criticidad en los activos del área de TI, ver tabla 8.

Tabla 8. Criterios de selección de la muestra

CRITERIO DE INCLUSIÓN	CRITERIO DE EXCLUSIÓN
La persona ejerce un puesto o cargo que se considera como "administrativo".	La persona ejerce un cargo que se considera como "operativo".
La persona se encuentra asignada a la sucursal de Honduras de Distribuidora Leterago.	La persona está asignada en otras sucursales diferentes a la de Honduras.
La persona forma parte activamente en los procesos administrativos de la empresa.	
La persona **no** forma parte del cuerpo investigativo.	La persona forma parte del desarrollo de la investigación.

Fuente: Elaboración propia.

También es necesario considerar que las personas que forman parte del desarrollo de la investigación no se deben incluir, por razones de sufrir un sesgo y dilemas éticos que podrían poner en compromiso la integridad de la investigación.

3.5 TÉCNICAS, INSTRUMENTOS Y PROCEDIMIENTOS APLICADOS

3.5.1 ANÁLISIS DE MÉTRICAS (MTTR)

- **TÉCNICA DE RECOLECCIÓN**

Se solicitará acceso al reporte sobre atención y soporte al usuario que genera la plataforma **Ticket** que la organización utiliza para sus operaciones diarias de gestión; este reporte posee información sobre la atención de diferentes situaciones o problemas que los usuarios finales experimentan por parte del equipo de TI que está en las oficinas.

La información en específico que se genera son los datos del usuario final como el nombre completo, correo asignado, motivo de solicitud de atención, fecha y hora del registro del incidente o situación. De parte del equipo de TI se genera información como la hora de atención del ticket, observaciones sobre la solución del incidente y la fecha y hora del cierre del ticket de atención.

Al obtener el reporte que contiene los ítems anteriormente mencionados, se procederá a hacer una limpieza de los datos utilizando diferentes herramientas; si bien el reporte se espera ser entregado en un archivo de Microsoft Excel, el propósito es poder exportarlo hacia una base de datos SQL, en donde se podrá hacer la normalización de datos (convertir ciertas columnas con otro tipo de datos), estandarización de registros (identificar filas duplicadas, filtrado de registros donde se encuentre información inconsistente o incompleta) y cálculos posteriores (tiempo promedio que toma atender a un usuario final desde el ingreso del ticket hasta su finalización).

- **INSTRUMENTO DE RECOLECCIÓN**

Creación de consulta SQL hacia tabla creada en base de datos parta poder traer los registros necesarios de manera ordenada y estandarizada según los lineamientos anteriormente establecidos (normalizar datos, estandarizar registros y hacer cálculos posteriores.

- **JUSTIFICACIÓN**

Esta técnica permitirá el cálculo de manera objetiva de la variable de eficiencia operativa, la cual se hace a raíz del cálculo del MTTR, de esta manera cumpliendo con el Objetivo Específico 3.

3.5.2 ENCUESTA ESTRUCTURADA

- **TÉCNICA DE RECOLECCIÓN**

Se creará una encuesta alojada en línea, dentro de la plataforma Microsoft Forms, será auto aplicable por medio de un enlace compartido por razones de agilidad.

La encuesta se diseñará con el propósito de medir conocimientos generales sobre la gestión de riesgos de la seguridad de la información mediante preguntas orientadas al nivel de concientización sobre el uso de las tecnologías que la organización provee, la medición sobre las experiencias y prácticas que los usuarios tienen en cuanto a la manera en la que ejecutan medidas de seguridad y de contingencia, y, por último, la perspectiva que los usuarios tienen para poder mejorar la manera en la que la empresa gestiona los riesgos. Es necesario tener en cuenta que se debe recolectar también generalidades como el área en donde el usuario labora y el tipo de sistemas con el que este interactúa.

- **INSTRUMENTO DE RECOLECCIÓN**

El cuestionario estructurado incluirá ítems con Escala de Likert de 5 puntos (brindando valoraciones de 1-5 donde el 1 es la cuantificación deficiente y el 5 es la cuantificación más satisfactoria) y preguntas con enfoque cualitativo orientadas a respuesta breve. Para ver el instrumento completo consultar el Anexo 3.

Al delimitar la información que se espera recibir del instrumento en diferentes ideas principales que corresponden a la asociación de las preguntas y objetivos con lo investigado en el marco teórico, es posible definir las secciones que comprenderá la encuesta, divididas de esta manera:

- **Sección 1:** Datos Generales
- **Sección 2:** Conocimiento y Concientización
- **Sección 3:** Evaluación de Competencias
- **Sección 4:** Experiencias y Prácticas
- **Sección 5:** Comentarios y Sugerencias

Para la **Sección 1** se recolectará información como el área en la que el usuario o sujeto de estudio labora, así como los sistemas que utiliza en su día a día, retratado por las siguientes preguntas de tipo selección:

- *Departamento en el que trabaja:*
  - Administración y Finanzas
  - Comercial
  - Personas y Cultura
  - Regencia y Calidad
  - Visitas Médicas
  - Gerencia
  - Otro
- *¿Qué tipo de sistemas de TI utiliza regularmente en sus labores diarias? (Seleccione todas las que apliquen)*

- ERP (Sistema de Planificación de Recursos Empresariales, como ser Microsoft Dynamics)
- Plataforma de correo electrónico (Outlook, Gmail)
- Herramientas de oficina (Suite de Microsoft Office)
- Otro

Para la **Sección 2** se recolectará información que concierne al nivel de conocimiento que el sujeto de estudio posee a nivel general sobre la gestión de riesgos por medio de la valoración o prioridad que este le dé a diferentes situaciones o afirmaciones que se plantean sobre el manejo de tecnologías y ciberseguridad, retratadas por las siguientes preguntas que utilizan la Escala de Likert anteriormente mencionada en el primer párrafo:

- *Siguiendo una escala del 1 al 5, donde 1 representa "Nada Importante" y 5 representa "Muy Importante", califique las siguientes afirmaciones según su criterio personal:*
  - ***La ciberseguridad y la gestión de riesgos de TI para contribuir a la eficiencia operativa de la empresa.***
  - ***La ciberseguridad debe ser para proteger los datos de clientes y proveedores.***
  - ***Se debe contar con un plan de recuperación ante desastres orientados al área de TI.***
  - ***Capacitar continuamente al personal en riesgos cibernéticos.***
- *Siguiendo una escala del 1 al 5, donde 1 representa "Nada Urgente" y 5 representa "Muy Urgente", califique las siguientes situaciones según su criterio personal:*
  - ***Un ataque de ransomware que bloquee el acceso a los sistemas de pedidos e inventario.***
  - ***Una filtración de datos confidenciales de clientes o productos.***
  - ***La caída prolongada del sistema ERP, impidiendo facturar o gestionar envíos.***

- ***El error humano interno (ej.: enviar un correo importante a la persona equivocada).***
- ***El incumplimiento de regulaciones farmacéuticas (ej.: trazabilidad de medicamentos).***

Para la **Sección 3** se evaluarán las competencias que se tienen acerca de la gestión de TI a nivel técnico, evaluado por medio de 3 preguntas de respuesta abierta cuyo propósito es que la muestra identifique componentes y procesos que se relacionan con la gestión de TI. Las respuestas servirán para posteriormente ser calificadas dentro de una matriz de competencias que permita traducir los dominios de la norma ISO 27005 en ítems y habilidades observables para la consideración de este estudio y del equipo de TI.

- *Liste 3 activos tecnológicos clave de la empresa y describa los riesgos asociados a la confidencialidad, integridad y disponibilidad.*
- *¿Qué proceso seguiría en caso de detectar un virus dentro de los sistemas de la empresa (considere el ERP, el almacenamiento en la nube o las carpetas compartidas)? Detalle paso a paso su forma de evaluar el riesgo y las acciones que tomaría.*
- *En el caso hipotético de que un excompañero de trabajo filtre información sensible de la empresa, proponga 3 controles para tratar esta situación. (Tome en cuenta 3 tipos de tratamiento: Preventivo, Detección y Correctivo).*

El resultado de estas respuestas, posteriormente calificadas manualmente por medio de una escala de 1 a 5, donde 1 es nulo y 5 es experto en la temática, se considerarán para el llenado de la matriz a continuación, ver tabla 9:

Tabla 9. Metodología de calificación del nivel de competencia por dominio ISO 27005

Dominio de ISO 27005	Competencia a Evaluar	Nivel de Competencia (1-5)	Evidencia a considerar
Establecimiento del Contexto	Identificar y documentar activos de información críticos del área		Se solicitará al evaluado listar 3 activos clave y describir los riesgos asociados a su

Dominio de ISO 27005	Competencia a Evaluar	Nivel de Competencia (1-5)	Evidencia a considerar
	administrativa.		confidencialidad, integridad y disponibilidad.
Análisis de Riesgo	Aplicar técnicas para estimar la probabilidad y el impacto de amenazas identificadas (como ser correos con phishing o ransomware).		El evaluado deberá explicar el proceso que seguiría para evaluar un nuevo tipo de malware que afecta al ERP.
Tratamiento del Riesgo	Conocimiento en la selección y justificación de controles de seguridad para mitigar riesgos.		Presentar un escenario de riesgo (ej. fuga de datos por un exempleado) y pedir que proponga 3 controles de tratamiento (preventivo, detección, correctivo).

Fuente: Elaboración propia

El proceso manual de calificación de estos ítems depende del conocimiento mostrado por los encuestadores para poder valorar estas preguntas.

Para la **Sección 4** se recolectará información sobre lo que el usuario ha experimentado en el área laboral orientado a la seguridad informática, así como los riesgos asociados a este y qué tipo de experiencia tiene con medidas de gestión de riesgos como planes de contingencia, retratado por las siguientes preguntas de tipo selección única:

- ***¿Ha recibido formación sobre cómo detectar amenazas de ciberseguridad como phishing o malware?***
  - Sí, de forma regular y actualizada.
  - Sí, pero hace mucho tiempo
  - No, nunca.
  - No estoy seguro/a.

- ***En el último año, ¿ha experimentado o presenciado algún incidente relacionado con la seguridad de la información? (ej.: correo phishing, ransomware, caída de sistemas críticos, pérdida de datos)***
    - Sí, en múltiples ocasiones.
    - Sí, en una ocasión.
    - No, nunca.
    - Prefiero no responder.
- ***Si respondió "Sí" a la pregunta anterior, ¿cómo manejó o reportó el incidente?***
    - Reporté inmediatamente al departamento de TI.
    - Lo reporté a mi supervisor/a
    - Intenté resolverlo por mi cuenta.
    - No supe qué hacer / No lo reporté.
    - No aplica.
- ***¿Con qué frecuencia realiza copias de seguridad (backups) de la información crítica de su trabajo hacia su directorio de nube asignado?***
    - Diariamente
    - Semanalmente
    - Mensualmente
    - Solo cuando me lo indican
    - Nunca / No sé cómo hacerlo

Para la **Sección 4** se recolectarán las opiniones y percepciones que el usuario tiene sobre la gestión de riesgos de seguridad de la información orientado a la manera en la que la empresa puede implementar o mejorar como retroalimentación, siendo esta parte cualitativa con preguntas abiertas que pretenden obtener un discernimiento mayor del sujeto de estudio, retratado por lo siguiente:

- ***Desde su perspectiva, ¿cuál es el mayor riesgo de TI al que se enfrenta nuestra***

empresa?

- ***¿Qué tipo de apoyo, recursos o capacitación cree que necesita para contribuir mejor a la seguridad de la información de la empresa?***

- **JUSTIFICACIÓN**

Esta técnica permitirá obtener datos cuantitativos y cualitativos que corresponden a la percepción que tiene la muestra sobre el nivel de conocimiento sobre la gestión de riesgos de la seguridad de la información en el área de TI y la identificación de factores organizacionales que pueden contribuir a la posible brecha de conocimiento sobre el tema, de esta manera dándole respuesta a los Objetivos Específicos 1 y 2.

- **VALIDACIÓN DEL INSTRUMENTO**

3.6 FUENTES DE INFORMACIÓN

Las fuentes de información corresponden a todos los datos que se recolectarán directa o indirectamente para satisfacer la necesidad de explorar la problemática de la investigación.

3.6.1 FUENTES PRIMARIAS

- **BASE DE DATOS DE RESPUESTAS A LA ENCUESTA**

La base de datos de respuesta a la encuesta aplicada es el resultado de la recopilación de todas las respuestas que sean ingresadas a la plataforma de Microsoft Forms y que, posteriormente, será parte de una estrategia de limpieza de datos para tener un set de datos íntegro y confiable.

Esta fuente tiene como propósito la exploración y análisis de las partes cuantitativa y cualitativa de la investigación que permitirán responder los Objetivos Específicos 1 y 2.

- **REPORTES DE ATENCIÓN DE TICKETS**

Se solicitará acceso a los reportes de atención de tickets ingresados por los usuarios finales, los cuales están alojados dentro de la plataforma **Tickets** y que alojan fechas y horas que permitirán la medición del MTTR. Para poder analizar y encontrar información valiosa que concierne a la investigación, será necesario procesarlos por medio de diferentes herramientas tecnológicas que permitan hacer una limpieza y cálculos posteriores en base a los datos obtenidos.

Esta fuente tiene como propósito la exploración y análisis de la parte cuantitativa de la investigación que permitirá responder el **Objetivo Específico 3**, así como tener una pieza más en

el panorama de percepción de la muestra contra los datos obtenidos.

- **RECOLECCIÓN DE DOCUMENTOS INSTITUCIONALES**

Se solicitará acceso a documentos de uso institucional que esté relacionado a la seguridad informática o la gestión de riesgos de activos del área de TI, como ser **políticas de seguridad, manuales de procedimientos e informes de seguridad.**

Esta fuente tiene como propósito contrastar lo recolectado en la base de datos de respuestas a la encuesta con lo documentado por la organización, que se puede considerar una realidad establecida dentro de su cultura organizacional.

3.6.2 FUENTES SECUNDARIAS

- **LITERATURA ACADÉMICA**

Se consultarán tanto artículos publicados en revistas de investigación como libros académicos en los cuales se podrá obtener un "estado del arte", refiriéndose a retratar un estado actual sobre el campo del que se está desarrollando la investigación. Estas diversas literaturas consultadas se verán anexadas dentro de la Bibliografía.

El propósito de utilizar esta fuente es para poder sentar las bases teóricas y metodológicas sobre las que reposa la validez e integridad de la investigación tomando diferentes referencias que puedan presentar una visión holística e integral del problema y su resolución.

- **MARCOS DE REFERENCIA**

Se utilizará como referencia para evaluar la gestión de riesgos como tal, la normativa ISO 27005, la cual proporciona lineamientos para la gestión de riesgos de seguridad de la información y permitirá comparar lo que se recolecte en los documentos institucionales como las políticas de seguridad y manuales de procedimientos con lo que plantea el marco de referencia, de esta manera satisfaciendo el Objetivo General y el Objetivo Específico 1.

El propósito de utilizar esta fuente es para poder sentar las bases teóricas y metodológicas sobre las que reposa la validez e integridad de la investigación tomando diferentes referencias que puedan presentar una visión holística e integral del problema y su resolución.

3.7 PLAN DE ANÁLISIS

A continuación, se detallan las actividades a realizar para la ejecución de la investigación,

partiendo desde la etapa de recolección de los datos hasta el análisis como tal.

Se considerarán 3 fases principales para la ejecución de este aspecto de la investigación, dentro de las cuales estarán las diferentes actividades que son necesarias para el cumplimiento de cada una de las fases; se divide en:

- **Preparación y Recolección de Fuentes**
    - **Diseño de la encuesta**

El diseño de la encuesta tiene como propósito producir un entregable como el instrumento de recolección validado; es una tarea que se realizará con las bases en las preguntas y objetivos de investigación relacionando lo visto en el marco teórica para poder formular preguntas que permitan medir los conocimientos que las personas tomadas de la muestra tienen sobre la gestión de riesgos para el área de TI.

Tiempo de duración: *2 semanas*

Puesto en el cronograma tentativo de cumplimiento: *Mes 1: Semana 1 – Semana 2.*

- **Extracción de reporte para medición de MTTR**

La actividad de la extracción del reporte sobre atención y soporte al usuario final que se genera en la plataforma Tickets empieza con la solicitud de acceso a los datos, mediante lo cual se extraerá una parte en específica delimitando el área de estudio; considerando que esta plataforma se utiliza por toda la organización en todas sus sucursales y atendiendo al diseño que investigación que se está implementando, es necesario delimitar el alcance de este, para lo cual solamente se considerarán los registros que involucren la sucursal de Honduras dentro del año 2025.

Tiempo de duración: 1 semana

Puesto en el cronograma tentativo de cumplimiento: *Mes 1: Semana 3.*

- **Limpieza de datos del reporte de atención de Tickets**

La actividad de limpieza de datos del reporte posterior a su extracción corresponde a una necesidad de poder procesar los datos de una manera clara y ordenada para evitar un sesgo u otros errores de procesamiento, dentro de lo cual se debe buscar la eliminación de inconsistencias, datos repetidos, datos que podrían no ser relevantes para el estudio, así como el filtrado y el ordenamiento para cumplir la delimitación poblacional de este estudio.

Se utilizará Microsoft Excel junto con su herramienta anexada Power Query para poder realizar este proceso, de lo cual se espera que se desarrolle en una semana para poder hacer pruebas y verificar la integridad de estos datos

Tiempo de duración: 1 semana

Puesto en el cronograma tentativo de cumplimiento: *Mes 1: Semana 4.*

- **Validación de la encuesta**

Considerando que el objetivo en esta etapa es evaluar elementos como la claridad, comprensión, tiempo de respuesta promedio y la valoración técnica del instrumento, se realizará una prueba pilotaje con 5 a 10 personas que finalmente no formen parte de la muestra seleccionada para el estudio, siempre formando parte del personal administrativo de Distribuidora Leterago y Laboratorios Megalabs.

Para la prueba pilotaje se utilizó el instrumento mostrado en el **Anexo 3**, que corresponde al bosquejo inicial del instrumento de recolección de datos, dentro de lo cual se encontró que 4 empleados prefirieron realizar la encuesta en formato físico, con el mensaje general de estar acostumbrados al medio y percibir que utilizar la plataforma de Microsoft Forms se les complicaba.

De la Sección 4 se cambiaron de orden las preguntas “Desde su perspectiva, ¿cuál es el mayor riesgo de TI al que se enfrenta nuestra empresa?” y “¿Qué tipo de apoyo, recursos o capacitación cree que necesita para contribuir mejor a la seguridad de la información de la empresa?”, por razones de claridad y secuencia.

Para obtener opiniones de expertos, se consultó con el asesor académico y el jefe del área de TI de Distribuidora Leterago para obtener perspectivas especializadas sobre la aplicación de la encuesta, la estructura del contenido y la precisión sobre la terminología plasmada, por lo cual se recibieron varias correcciones de secuencias en las preguntas en la sección 4, y la evaluación de la sección cualitativa, la cual se agregó para poder evaluar los dominios que corresponden a la norma ISO 27005, así como dentro de ella hacer ajustes y usar terminología clara para mantener un nivel de objetividad sobre la calificación posterior que los investigadores realizarán, como se ve reflejado en el **Anexo 4.**

Tiempo de duración: 1 semana

Puesto en el cronograma tentativo de cumplimiento: *Mes 2: Semana 1.*

- **Aplicación de la encuesta**

De la aplicación de la encuesta corresponde a la distribución y promoción del instrumento de recolección de datos dirigido hacia la muestra, que en este caso son los empleados de índole administrativa que laboran en Distribuidora Leterago.

Se planea compartir y socializar el enlace de la encuesta por medio de canales de comunicación oficiales, como ser Microsoft Teams y el correo de Outlook, dentro de lo cual se espera que toda la muestra que se delimitó pueda llenar el instrumento en un lapso de 2 semanas.

Tiempo de duración: 2 semanas

Puesto en el cronograma tentativo de cumplimiento: *Mes 2: Semana 2 – 3.*

- **Análisis Preliminar**
  - **Análisis exploratorio de los datos**

El análisis exploratorio de los datos dentro de la parte preliminar implica la revisión a un nivel semi superficial de las variables y categorizar lo que se ha recibido hasta el momento; el diseño de diferentes gráficos, tablas resumen y otras inferencias que se podrían obtener en base a los datos recibidos empieza en esta etapa, donde se empieza a materializar el bosquejo del resultado esperado.

Tiempo de duración: 1 semana

Puesto en el cronograma tentativo de cumplimiento: *Mes 2: Semana 4.*

- **Análisis Final e Investigación**
  - **Análisis temático de la parte cualitativa de la encuesta para identificar categorías emergentes**

El análisis temático de la parte cualitativa se refiere a la identificación de categorías emergentes que se podrían encontrar en base a las respuestas; de qué manera la relación de estas categorías afecta a las variables de estudio y qué tipo de inferencias se pueden ir formando para finalmente crear conclusiones y recomendaciones.

Tiempo de duración: 2 semanas

Puesto en el cronograma tentativo de cumplimiento: *Mes 3: Semana 1 – 2.*

- **Triangulación de datos cuantitativos y cualitativos**

Triangular datos cuantitativos y cualitativos significa encontrar las relaciones entre los gráficos creados en la parte del análisis exploratorio contra la relación que podrían tener las categorías emergentes al haber analizado de manera temática la parte cualitativa de la encuesta y la documentación existente de la organización, como sus manuales de procesos y otros históricos. Esto permitirá tener un mejor panorama de todo el fenómeno y de esta manera poder construir conclusiones y recomendaciones que estén fundamentadas en datos tangibles, verificables e íntegros.

Tiempo de duración: 2 semanas

Puesto en el cronograma tentativo de cumplimiento: *Mes 3: Semana 3 – 4.*

- **Redacción del Capítulo 4: Resultados y Análisis**

Todas las actividades realizadas anteriormente dentro del plan de análisis conllevan finalmente a la redacción del capítulo cuatro donde se estructurará todo lo he encontrado coma todo lo he estudiado para poder generar un panorama robusto detallado y que permita entender el fenómeno y darle respuestas a las variables que se están estudiando.

Se deberá mostrar todo lo encontrado (manuales de proceso, reportes, respuestas cualitativas del instrumento y datos históricos de la organización) junto con lo producido (gráficos) para poder dejar bien fundamentado lo que se quiere analizar, decir y por último concluir acerca del fenómeno de estudio.

Tiempo de duración: 2 semanas

Puesto en el cronograma tentativo: *Mes 4: Semana 1 – Mes 4: Semana 2.*

Se utilizará una tabla basada en principios de gestión de proyectos para sintetizar todos los componentes de estas actividades y cómo es posible distribuirlas a lo largo del tiempo. Ver tabla 10.

Tabla 10. Plan de Análisis una vez aplicado el instrumento de investigación

FASE	ACTIVIDAD A REALIZAR	ENTREGABLE	DURACIÓN (EN SEMANAS)	CRONOGRAMA TENTATIVO DE CUMPLIMIENTO
Preparación y Recolección de Fuentes	Diseño de la encuesta.	Instrumento de recolección	2	Mes 1: Semana 1 – 2.
	Extracción de reporte de atención de Tickets para medición de MTTD y MTTR.	Set de datos que contiene los campos para el cálculo de métricas	1	Mes 1: Semana 3.
	Limpieza de datos del reporte de atención de Tickets	Set de datos que contiene la medición de tiempos normalizado	1	Mes 1: Semana 4
	Validación de encuesta	Instrumento de recolección validado.	1	Mes 2: Semana 1.
	Aplicación de la encuesta.	Base de datos de respuestas.	2	Mes 2: Semana 2 – 3.
Análisis Preliminar	Análisis exploratorio de los datos.	Reporte descriptivo.	1	Mes 2: Semana 4. Mes 3: Semana 1.
Análisis Final e Investigación	Análisis temático de la parte cualitativa de la encuesta para identificar categorías emergentes.	Matriz temática	2	Mes 3: Semana 2 – 3.
	Triangulación de datos cuantitativos y cualitativos.	Matriz de inferencias multidimensional.	2	Mes 3: Semana 4. Mes 4: Semana 1.
	Redacción del Capítulo 4: Resultados y Análisis.	Borrador Completo de Capítulo 4	2	Mes 4: Semana 2 – 3.

Fuente: Elaboración propia.

CAPÍTULO IV. RESULTADOS Y ANÁLISIS

El presente capítulo se centra en el **Análisis Exploratorio de Datos** (EDA) que es considerado una de las fases más relevantes del proceso de investigación, ya que a través de este es posible llevar a cabo una interpretación a profundidad de la naturaleza, estructura y calidad de la información obtenida. Por medio de este se pretende dar a conocer patrones, tendencias, valores

atípicos y relaciones evidentes entre las variables para poder garantizar la validez y la consistencia de los datos antes del desarrollo de análisis estadísticos o modelados más avanzados.

Para dar cumplimiento a la realización del EDA se utilizará el software KNIME que es una herramienta de análisis visual, lo que permite el tratamiento sistemático y reproducible de grandes cantidades de datos por medio de flujos de trabajo modulares. Su entorno basado en nodos permite llevar a cabo los procesos de lectura, depuración, transformación y visualización de los datos sin la necesidad de poseer o adquirir conocimientos avanzados en programación.

Para el caso de esta etapa, se hará considerando los dos conjuntos de datos principales obtenidos para la investigación: el Reporte de Tickets mediante el cual se calcula el MTTR y las respuestas de la encuesta estructurada. Al MTTR se hará referencia como "Tiempo de Respuesta" o "Tiempo de Resolución Promedio" por razones de claridad.

4.1 ANÁLISIS EXPLORATORIO DE LOS DATOS

La siguiente sección tiene como propósito mostrar todos los datos importantes encontrados a la hora de explorar los sets de datos que corresponden al Reporte de Tickets y las respuestas de la encuesta estructurada.

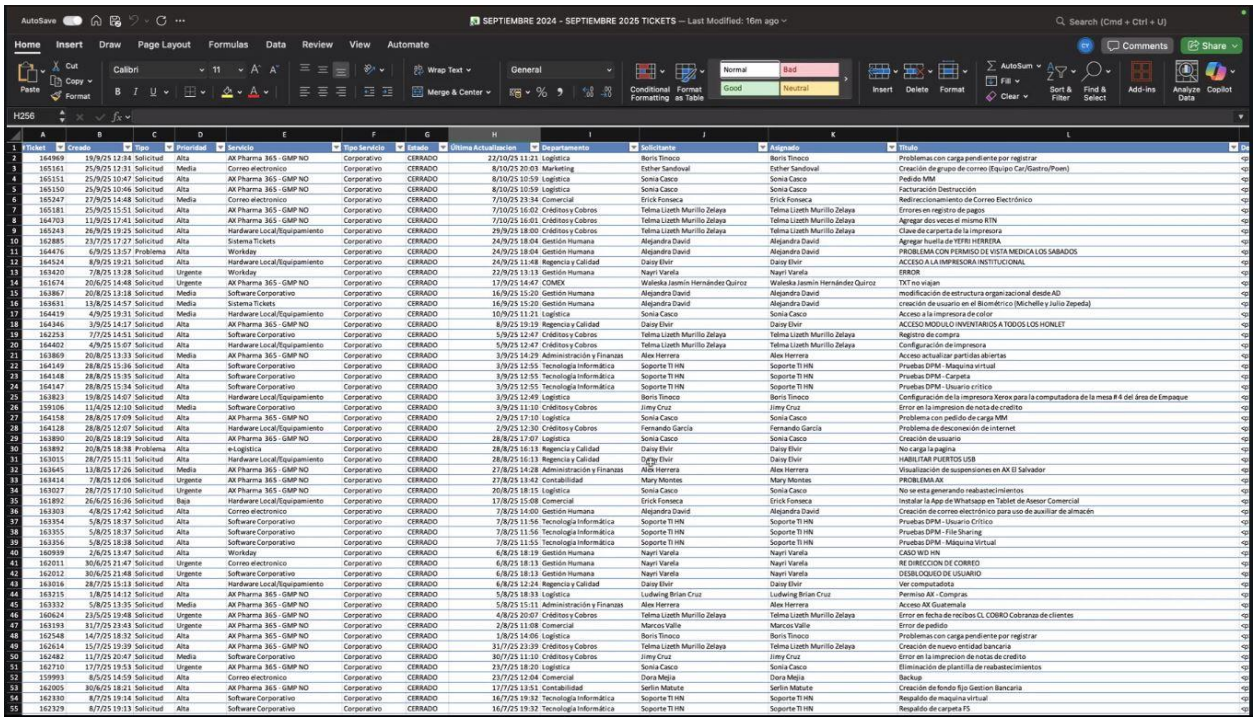
4.1.1 DESCRIPCIÓN GENERAL DEL CONJUNTO DE DATOS

- Reporte de Tickets

El reporte de Tickets atendidos por el área de Tecnologías de la Información fue extraído utilizando un filtro de fecha con el que se busca delimitar el periodo de tiempo que se está estudiando, en este caso, del mes de **septiembre del año 2024 a septiembre del año 2025**.

Si bien el reporte original es mostrado solamente en el sistema de manejo de Tickets, es posible dentro de él, filtrar por diferentes campos, y, en este caso, se utilizó la fecha, teniendo como resultado **247 registros únicos**. La plataforma de tickets también permite descargar estos reportes directamente hacia un archivo de Excel, lo cual se muestra en la tabla 11:

Tabla 11. Historial de tickets septiembre 2024 – septiembre 2025



# Ticket	Creado	Tipo	Prioridad	Servicio	Tipo Servicio	Estado	Última Actualizacion	Departamento	Solicitante	Asignado	Titulo
164969	19/9/25 12:34	Solicitud	Alta	AX Pharma 365 - GMP NO	Corporativo	CERRADO	22/10/25 11:21	Logística	Boris Tinoco	Boris Tinoco	Problemas con carga pendiente por registrar
165161	25/9/25 12:31	Solicitud	Media	Correo electronico	Corporativo	CERRADO	8/10/25 20:03	Marketing	Esther Sandoval	Esther Sandoval	Creación de grupo de correo (Equipo Car/Gastro/Poem)
165151	25/9/25 10:47	Solicitud	Alta	AX Pharma 365 - GMP NO	Corporativo	CERRADO	8/10/25 10:59	Logística	Sonia Casco	Sonia Casco	Pedido MM
165150	25/9/25 10:46	Solicitud	Alta	AX Pharma 365 - GMP NO	Corporativo	CERRADO	8/10/25 10:59	Logística	Sonia Casco	Sonia Casco	Facturación Destrucción
165247	27/9/25 14:48	Solicitud	Media	Correo electronico	Corporativo	CERRADO	7/10/25 23:34	Comercial	Erick Fonseca	Erick Fonseca	Redirecccionamiento de Correo Electrónico
165181	25/9/25 15:51	Solicitud	Alta	AX Pharma 365 - GMP NO	Corporativo	CERRADO	7/10/25 16:02	Créditos y Cobros	Telma Lizeth Murillo Zelaya	Telma Lizeth Murillo Zelaya	Errores en registro de pagos
164703	11/9/25 17:41	Solicitud	Alta	AX Pharma 365 - GMP NO	Corporativo	CERRADO	7/10/25 16:01	Créditos y Cobros	Telma Lizeth Murillo Zelaya	Telma Lizeth Murillo Zelaya	Agregar dos veces el mismo RTN
165243	26/9/25 19:25	Solicitud	Alta	Hardware Local/Equipamiento	Corporativo	CERRADO	29/9/25 18:00	Créditos y Cobros	Telma Lizeth Murillo Zelaya	Telma Lizeth Murillo Zelaya	Clave de carpeta de la impresora
162885	23/7/25 17:27	Solicitud	Alta	Sistema Tickets	Corporativo	CERRADO	24/9/25 18:04	Gestión Humana	Alejandra David	Alejandra David	Agregar huella de YEFRI HERRERA
164476	6/9/25 13:57	Problema	Alta	Workday	Corporativo	CERRADO	24/9/25 18:04	Gestión Humana	Alejandra David	Alejandra David	PROBLEMA CON PERMISO DE VISTA MEDICA LOS SABADOS
164524	8/9/25 19:21	Solicitud	Alta	Hardware Local/Equipamiento	Corporativo	CERRADO	24/9/25 11:48	Regencia y Calidad	Daisy Elvir	Daisy Elvir	ACCESO A LA IMPRESORA INSTITUCIONAL
163420	7/8/25 13:28	Solicitud	Urgente	Workday	Corporativo	CERRADO	22/9/25 13:13	Gestión Humana	Nayri Varela	Nayri Varela	ERROR
161674	20/6/25 14:48	Solicitud	Urgente	AX Pharma 365 - GMP NO	Corporativo	CERRADO	17/9/25 14:47	COMEX	Waleska Jasmín Hernández Quiroz	Waleska Jasmín Hernández Quiroz	TXT no viajan
163867	20/8/25 13:18	Solicitud	Media	Software Corporativo	Corporativo	CERRADO	16/9/25 15:20	Gestión Humana	Alejandra David	Alejandra David	modificación de estructura organizacional desde AD
163631	13/8/25 14:57	Solicitud	Media	Sistema Tickets	Corporativo	CERRADO	16/9/25 15:20	Gestión Humana	Alejandra David	Alejandra David	creación de usuario en el Biométrico (Michelle y Julio Zepeda)
164419	4/9/25 19:31	Solicitud	Media	Hardware Local/Equipamiento	Corporativo	CERRADO	10/9/25 11:21	Logística	Sonia Casco	Sonia Casco	Acceso a la impresora de color
164346	3/9/25 14:17	Solicitud	Alta	AX Pharma 365 - GMP NO	Corporativo	CERRADO	8/9/25 19:19	Regencia y Calidad	Daisy Elvir	Daisy Elvir	ACCESO MODULO INVENTARIOS A TODOS LOS HONLET
162253	7/7/25 14:51	Solicitud	Alta	Software Corporativo	Corporativo	CERRADO	5/9/25 12:47	Créditos y Cobros	Telma Lizeth Murillo Zelaya	Telma Lizeth Murillo Zelaya	Registro de compra
164402	4/9/25 15:07	Solicitud	Alta	Hardware Local/Equipamiento	Corporativo	CERRADO	5/9/25 12:47	Créditos y Cobros	Telma Lizeth Murillo Zelaya	Telma Lizeth Murillo Zelaya	Configuración de impresora
163869	20/8/25 13:33	Solicitud	Media	AX Pharma 365 - GMP NO	Corporativo	CERRADO	3/9/25 14:29	Administración y Finanzas	Alex Herrera	Alex Herrera	Acceso actualizar partidas abiertas
164149	28/8/25 15:36	Solicitud	Alta	Software Corporativo	Corporativo	CERRADO	3/9/25 12:55	Tecnología Informática	Soporte TI HN	Soporte TI HN	Pruebas DPM - Maquina virtual
164148	28/8/25 15:35	Solicitud	Alta	Software Corporativo	Corporativo	CERRADO	3/9/25 12:55	Tecnología Informática	Soporte TI HN	Soporte TI HN	Pruebas DPM - Carpeta
164147	28/8/25 15:34	Solicitud	Alta	Software Corporativo	Corporativo	CERRADO	3/9/25 12:55	Tecnología Informática	Soporte TI HN	Soporte TI HN	Pruebas DPM - Usuario crítico
163823	19/8/25 14:07	Solicitud	Alta	Hardware Local/Equipamiento	Corporativo	CERRADO	3/9/25 12:49	Logística	Boris Tinoco	Boris Tinoco	Configuración de la impresora Xerox para la computadora de la mesa # 4 del área de Empaque
159106	11/4/25 12:10	Solicitud	Media	Software Corporativo	Corporativo	CERRADO	3/9/25 11:10	Créditos y Cobros	Jimy Cruz	Jimy Cruz	Error en la impresion de nota de credito
164158	28/8/25 17:09	Solicitud	Alta	AX Pharma 365 - GMP NO	Corporativo	CERRADO	2/9/25 17:10	Logística	Sonia Casco	Sonia Casco	Problema con pedido de carga MM
164128	28/8/25 12:07	Solicitud	Alta	Hardware Local/Equipamiento	Corporativo	CERRADO	2/9/25 12:30	Créditos y Cobros	Fernando García	Fernando García	Problema de desconexión de internet
163890	20/8/25 18:19	Solicitud	Alta	AX Pharma 365 - GMP NO	Corporativo	CERRADO	28/8/25 17:07	Logística	Sonia Casco	Sonia Casco	Creación de usuario
163892	20/8/25 18:38	Problema	Alta	e-Logistica	Corporativo	CERRADO	28/8/25 16:13	Regencia y Calidad	Daisy Elvir	Daisy Elvir	No carga la pagina
163015	28/7/25 15:11	Solicitud	Alta	Hardware Local/Equipamiento	Corporativo	CERRADO	28/8/25 16:13	Regencia y Calidad	Daisy Elvir	Daisy Elvir	HABILITAR PUERTOS USB
163645	13/8/25 17:26	Solicitud	Media	AX Pharma 365 - GMP NO	Corporativo	CERRADO	27/8/25 14:28	Administración y Finanzas	Alex Herrera	Alex Herrera	Visualización de suspensiones en AX El Salvador
163414	7/8/25 12:06	Solicitud	Urgente	AX Pharma 365 - GMP NO	Corporativo	CERRADO	27/8/25 13:42	Contabilidad	Mary Montes	Mary Montes	PROBLEMA AX
163027	28/7/25 17:10	Solicitud	Urgente	AX Pharma 365 - GMP NO	Corporativo	CERRADO	20/8/25 18:15	Logística	Sonia Casco	Sonia Casco	No se esta generando reabastecimientos
161892	26/6/25 16:36	Solicitud	Baja	Hardware Local/Equipamiento	Corporativo	CERRADO	17/8/25 15:08	Comercial	Erick Fonseca	Erick Fonseca	Instalar la App de Whatsapp en Tablet de Asesor Comercial
163303	4/8/25 17:42	Solicitud	Alta	Correo electronico	Corporativo	CERRADO	7/8/25 14:00	Gestión Humana	Alejandra David	Alejandra David	Creación de correo electrónico para uso de auxiliar de almacén
163354	5/8/25 18:37	Solicitud	Alta	Software Corporativo	Corporativo	CERRADO	7/8/25 11:56	Tecnología Informática	Soporte TI HN	Soporte TI HN	Pruebas DPM - Usuario Crítico
163355	5/8/25 18:37	Solicitud	Alta	Software Corporativo	Corporativo	CERRADO	7/8/25 11:56	Tecnología Informática	Soporte TI HN	Soporte TI HN	Pruebas DPM - File Sharing
163356	5/8/25 18:38	Solicitud	Alta	Software Corporativo	Corporativo	CERRADO	7/8/25 11:55	Tecnología Informática	Soporte TI HN	Soporte TI HN	Pruebas DPM - Máquina Virtual
160939	2/6/25 13:47	Solicitud	Alta	Workday	Corporativo	CERRADO	6/8/25 18:19	Gestión Humana	Nayri Varela	Nayri Varela	CASO WD HN
162011	30/6/25 21:47	Solicitud	Urgente	Correo electronico	Corporativo	CERRADO	6/8/25 18:13	Gestión Humana	Nayri Varela	Nayri Varela	RE DIRECCION DE CORREO
162012	30/6/25 21:48	Solicitud	Urgente	Software Corporativo	Corporativo	CERRADO	6/8/25 18:13	Gestión Humana	Nayri Varela	Nayri Varela	DESBLOQUEO DE USUARIO
163016	28/7/25 15:13	Solicitud	Alta	Hardware Local/Equipamiento	Corporativo	CERRADO	6/8/25 12:24	Regencia y Calidad	Daisy Elvir	Daisy Elvir	Ver computadota
163215	1/8/25 14:12	Solicitud	Alta	AX Pharma 365 - GMP NO	Corporativo	CERRADO	5/8/25 18:33	Logística	Ludwing Brian Cruz	Ludwing Brian Cruz	Permiso AX - Compras
163332	5/8/25 13:35	Solicitud	Media	AX Pharma 365 - GMP NO	Corporativo	CERRADO	5/8/25 15:11	Administración y Finanzas	Alex Herrera	Alex Herrera	Acceso AX Guatemala
160624	23/5/25 19:48	Solicitud	Urgente	AX Pharma 365 - GMP NO	Corporativo	CERRADO	4/8/25 20:07	Créditos y Cobros	Telma Lizeth Murillo Zelaya	Telma Lizeth Murillo Zelaya	Error en fecha de recibos CL COBRO Cobranza de clientes
163193	31/7/25 23:43	Solicitud	Urgente	AX Pharma 365 - GMP NO	Corporativo	CERRADO	2/8/25 11:08	Comercial	Marcos Valle	Marcos Valle	Error de pedido
162548	14/7/25 18:32	Solicitud	Alta	AX Pharma 365 - GMP NO	Corporativo	CERRADO	1/8/25 14:06	Logística	Boris Tinoco	Boris Tinoco	Problemas con carga pendiente por registrar
162614	15/7/25 19:39	Solicitud	Alta	AX Pharma 365 - GMP NO	Corporativo	CERRADO	31/7/25 23:39	Créditos y Cobros	Telma Lizeth Murillo Zelaya	Telma Lizeth Murillo Zelaya	Creación de nuevo entidad bancaria
162482	11/7/25 20:47	Solicitud	Media	Software Corporativo	Corporativo	CERRADO	30/7/25 11:10	Créditos y Cobros	Jimy Cruz	Jimy Cruz	Error en la impresion de notas de credito
162710	17/7/25 19:53	Solicitud	Urgente	AX Pharma 365 - GMP NO	Corporativo	CERRADO	23/7/25 18:20	Logística	Sonia Casco	Sonia Casco	Eliminación de plantilla de reabastecimientos
159993	8/5/25 14:59	Solicitud	Alta	Correo electronico	Corporativo	CERRADO	23/7/25 12:04	Comercial	Dora Mejia	Dora Mejia	Backup
162005	30/6/25 18:21	Solicitud	Alta	AX Pharma 365 - GMP NO	Corporativo	CERRADO	17/7/25 13:51	Contabilidad	Serlin Matute	Serlin Matute	Creación de fondo fijo Gestion Bancaria
162330	8/7/25 19:14	Solicitud	Alta	Software Corporativo	Corporativo	CERRADO	16/7/25 19:32	Tecnología Informática	Soporte TI HN	Soporte TI HN	Respaldo de maquina virtual
162329	8/7/25 19:13	Solicitud	Alta	Software Corporativo	Corporativo	CERRADO	16/7/25 19:32	Tecnología Informática	Soporte TI HN	Soporte TI HN	Respaldo de carpeta FS

Fuente: Elaboración propia con data de reportería de tickets local

Las variables a estudiar sean cualitativas o cuantitativas, se muestran en la tabla 12.

Tabla 12. Variables Analizadas del Reporte de Tickets:

Variable	Descripción	Tipo de Dato	Comentario (Si aplica)
# Ticket	Identificador único asignado a cada ticket o solicitud registrada.	Alfanumérico	Dato no relevante, es un identificador
Creado	Fecha y hora en que se generó el ticket.	Fecha	
Tipo	Clasificación del ticket según su naturaleza.	Texto	Limitado a, SOLICITUD o PROBLEMA
Prioridad	Nivel de urgencia o impacto del ticket.	Texto	Limitado a, BAJA, MEDIA, ALTA, URGENTE
Servicio	Servicio afectado o al que está asociado el ticket.	Texto	Limitado al nombre las plataformas/servicios internos más utilizados
Tipo Servicio	Subcategoría o especificación del servicio dentro del área TI.	Texto	Limitado a, CORPORATIVO o LOCAL
Estado	Situación actual del ticket dentro del flujo de atención.	Texto	Limitado a estado CERRADO
Última Actualización	Fecha de la última modificación o acción registrada en el ticket.	Fecha	
Departamento	Área o departamento solicitante.	Texto	Limitado al nombre de los departamentos locales

Variable	Descripción	Tipo de Dato	Comentario (Si aplica)
Solicitante	Nombre de la persona que generó el ticket.	Texto	Dato no relevante, nombres de personas
Asignado	Nombre de la persona que realizó la última actualización en el ticket.	Texto	Dato no relevante, nombres de personas
Título	Breve resumen del problema o solicitud.	Texto	Dato no relevante, es muy subjetivo (depende del razonamiento del usuario que ingresó el ticket)
Descripción	Detalle completo del problema o solicitud.	Texto (largo)	Dato no relevante, es muy subjetivo (depende del razonamiento del usuario que ingresó el ticket)
País-Empresa	País o entidad empresarial a la que pertenece el solicitante.	Texto	Limitado a, HN-Leterago o HN-Megalabs
Ubicación	Lugar físico o sede donde se originó el ticket.	Texto	Dato no relevante, limitado a solo TEGUCIGALPA
Resp. TI Local	Encargado local de soporte técnico.	Texto	Dato no relevante, limitado a solo SOPORTE TI HN
Resultado Encuesta	Evaluación del usuario posterior a la resolución (satisfacción).	Texto	Limitado a, INSATISFECHO, REGULAR, SATISFECHO, MUY SATISFECHO, EXCELENTE
Referencia	Campo auxiliar para notas o referencias internas.	Texto	Dato no relevante, es muy subjetivo (depende del razonamiento del usuario que ingresó el ticket)
Tiempo Resolución	Duración en horas total empleada en resolver el ticket.	Numérico	Resultado de la diferencia entre las variables: Última Actualización - Creado

Fuente: Elaboración propia.

Para poder realizar un estudio más puntual de las variables que los investigadores consideran más importantes para el estudio, se aplicó un Filtro de Columnas dentro del flujo de KNIME, por lo cual se delimitaron las variables que se estarán utilizando para los consiguientes gráficos. Véase la figura 7:

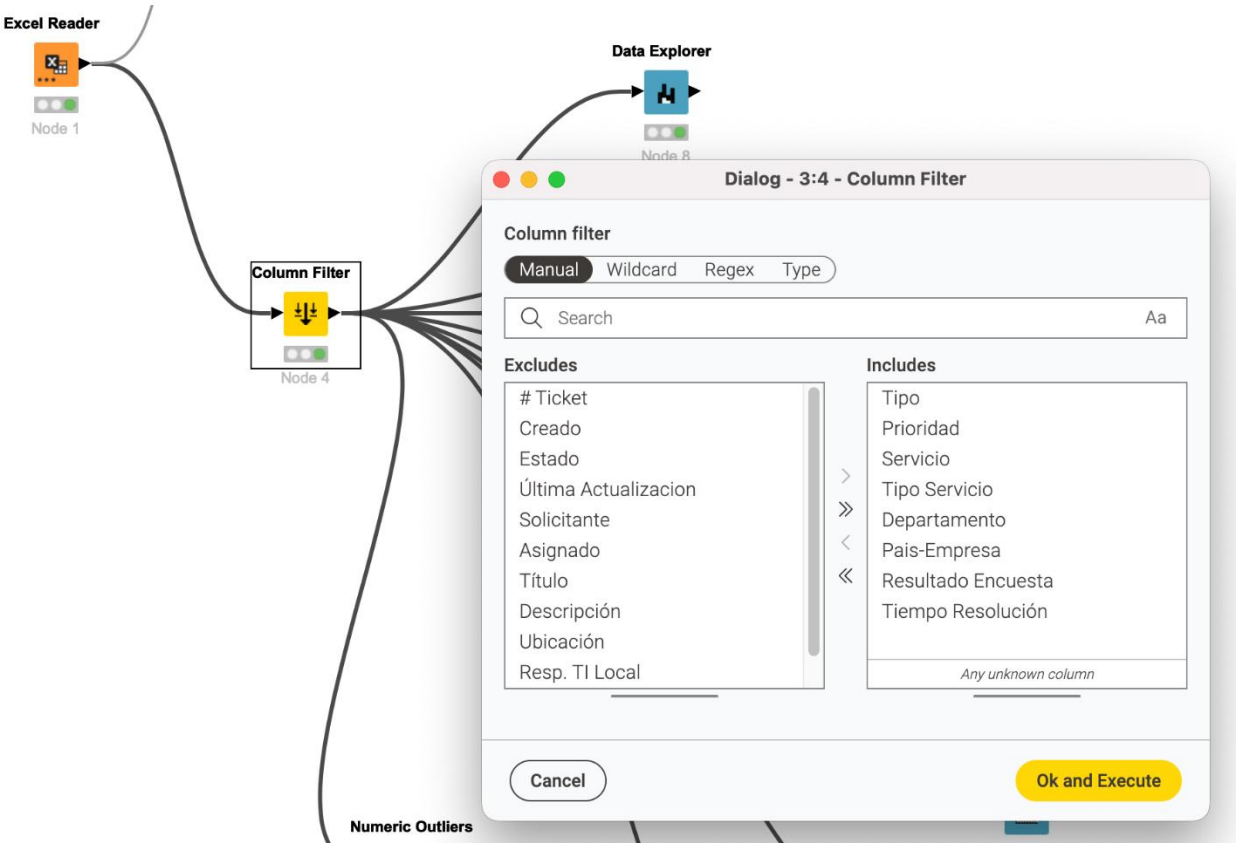


Figura 6. Delimitación de variables previo a análisis de datos en KNIME.

Fuente: Elaboración propia

La variable cuantitativa más importante del set de datos es **Tiempo Resolución**, el cual permitirá obtener el MTTR y, de igual manera, hacer diferentes estudios y generar gráficas que puedan dar un mejor panorama al fenómeno que se está estudiando. Para una mejor comprensión de la data recolectada en la tabla 13 se presentan los datos estadísticos básicos.

Tabla 13. Datos estadísticos MTTR

Datos estadísticos del Tiempo de Respuesta (MTTR)

Column	Minimum	Maximum	Mean	Median	Standard Deviation	Variance	Skewness	Kurtosis	Overall Sum	No. zeros	No. missings
Tiempo Resolución	0	3478.998	375.152	162.149	540.923	292598.017	2.942	10.560	93037.656	7	0

Fuente: Elaboración propia

La variable Tiempo Resolución posee un **mínimo de 0** y un **máximo de 3478.998 horas**, donde la media es **375.152** horas y su desviación estándar es de **540.923**; se encuentran 7 registros con valor 0 y ningún valor faltante.

En cuanto a las variables cualitativas, se encuentra que no se tiene ningún valor faltante en sus registros y corresponde a lo descrito en la Tabla 10, véase la siguiente tabla en donde se describen los valores únicos, su cantidad y una pequeña gráfica de barras que muestra la frecuencia de estos valores nominales. Ver tabla 14.

Tabla 14. **Análisis preliminar MTTR**

Datos estadísticos del Tiempo de Respuesta (MTTR)

Column	No. missings	Unique values	All nominal values	Frequency Bar Chart
Tipo	0	2	Solicitud, Problema	
Prioridad	0	4	Alta, Urgente, Media, Baja	
Servicio	0	13	AX Pharma 365 - GMP NO, Software Corporativo, Hardware Local/Equipamiento, Correo electronico, Workday, [...], GADE, Power BI CEAM, Sigma CRM, SAC, CVP	
Tipo Servicio	0	2	Corporativo, Local	
Departamento	0	11	Logística, Créditos y Cobros, Tecnología Informática, Contabilidad, Comercial, [...], Regencia y Calidad, Administración y Finanzas, COMEX, Mejora Continua, Marketing	
Pais-Empresa	0	2	HN-Leterago, HN-Megalabs	
Resultado Encuesta	0	4	Excelente, Sin encuestar, Muy Satisfecho, Satisfecho	

Fuente: Elaboración propia

- Respuestas de encuesta estructurada

Los resultados de la encuesta estructurada fueron extraídos directamente de la fuente, en este caso, Microsoft Forms, cuya plataforma almacena todas las entradas de la encuesta dentro de un archivo de Excel al que es posible acceder desde la carpeta de la nube de OneDrive y se actualiza automáticamente.

A continuación, en la tabla 15 se desglosa la lista completa de variables a tomar en cuenta para el estudio exploratorio.

Tabla 15. Variables Analizadas en la encuesta

Sección 1: Datos Generales

Variable	Descripción	Tipo de Dato	Valores o Categorías	Comentario (Si aplica)
Departamento	Departamento en el que trabaja el encuestado	Texto	1.Administración y Finanzas 2. Comercial 3. Personas y Cultura 4. Regencia y Calidad 5. Visitas Médicas 6. Gerencia 7. Otro (especificar)	Categórica nominal (Solo una opción)
Sistemas Utilizados	Tipo de sistemas/plataforma tecnológica que utiliza regularmente el encuestado	Texto	ERP / Correo electrónico / Herramientas de oficina / Otro	Categórica múltiple (Puede marcar varias opciones)
Rol Principal	Rol principal del encuestado en la organización	Texto	1. Liderazgo / Supervisión 2. Colaborador Técnico / Especializado 3. Colaborador Administrativo / Soporte	Categórica nominal (Solo una opción)

Sección 2: Conocimiento y Concientización

Variable	Descripción	Tipo	Comentario (Si aplica)
Eficiencia Operativa	Importancia de la ciberseguridad y gestión de riesgos TI para la eficiencia operativa	Numérico	Ordinal (1–5)
Protección de Datos	Importancia de proteger datos de clientes y proveedores	Numérico	Ordinal (1–5)
Recuperación	Importancia de contar con un plan de recuperación ante desastres TI	Numérico	Ordinal (1–5)
Capacitación	Importancia de capacitar al personal en riesgos cibernéticos	Numérico	Ordinal (1–5)
Ransomware	Urgencia ante un ataque de ransomware	Numérico	Ordinal (1–5)
Filtración de datos	Urgencia ante una filtración de datos confidenciales	Numérico	Ordinal (1–5)

Caída ERP	Urgencia ante la caída del sistema ERP	Numérico	Ordinal (1–5)
Error Humano	Urgencia ante un error humano (correo enviado erróneamente)	Numérico	Ordinal (1–5)
Incumplimiento Regulatorio	Urgencia ante incumplimiento de regulaciones farmacéuticas	Numérico	Ordinal (1–5)

Sección 3: Evaluación de Competencias

Variable	Descripción	Tipo	Comentario (Si aplica)
Activos Tecnológicos y Riesgos	Lista de 3 activos tecnológicos clave y sus riesgos de confidencialidad, integridad y disponibilidad	Texto	Respuesta cualitativa
Procedimiento Virus	Descripción del proceso que seguiría ante detección de virus	Texto	Respuesta cualitativa
Controles Filtración de Información	Propuesta de controles preventivos y correctivos ante fuga de información	Texto	Respuesta cualitativa

Sección 4: Experiencias y Prácticas

Variable	Descripción	Tipo	Valores o Categorías
Formación en ciberseguridad	Ha recibido formación para detectar amenazas de ciberseguridad	Categórica nominal	1. Sí, regular y actualizada 2. Sí, hace mucho tiempo 3. No, nunca 4. No está seguro/a
Experiencia en Incidentes	Ha presenciado incidentes de seguridad de la información en el último año	Categórica nominal	1. Sí, múltiples ocasiones 2. Sí, una ocasión 3. No, nunca 4. Prefiero no responder
Manejo Incidente	Cómo manejó o reportó el incidente	Categórica nominal	1. Reporté al TI 2. Reporté al supervisor/a 3. Intenté resolverlo 4. No supe qué hacer

			/ No lo reporté 5. No aplica
Frecuencia Backup	Frecuencia con la que realiza copias de seguridad	Categórica ordinal	1. Diariamente 2. Semanalmente 3. Mensualmente 4. Solo cuando me lo indican 5. Nunca / No sé cómo hacerlo

Sección 5: Comentarios y Sugerencias

Variable	Descripción	Tipo	Comentario (Si aplica)
Riesgo de TI Principal	Riesgo de TI que considera más importante para la empresa	Texto	Opinión libre
Necesidad de Capacitación	Tipo de apoyo o recursos que considera necesarios	Texto	Opinión libre

Fuente: Elaboración propia

Tomando en cuenta las variables especificadas en el diccionario, se deben excluir algunas columnas que vienen por defecto en el archivo de Excel que se exporta desde Microsoft Forms. Campos como el identificador único de fila, correo electrónico, nombre y variables de tipo texto no se incluirán, como lo mostrado en la figura 7 al utilizar KNIME para filtrar solamente las columnas que se consideran importantes.

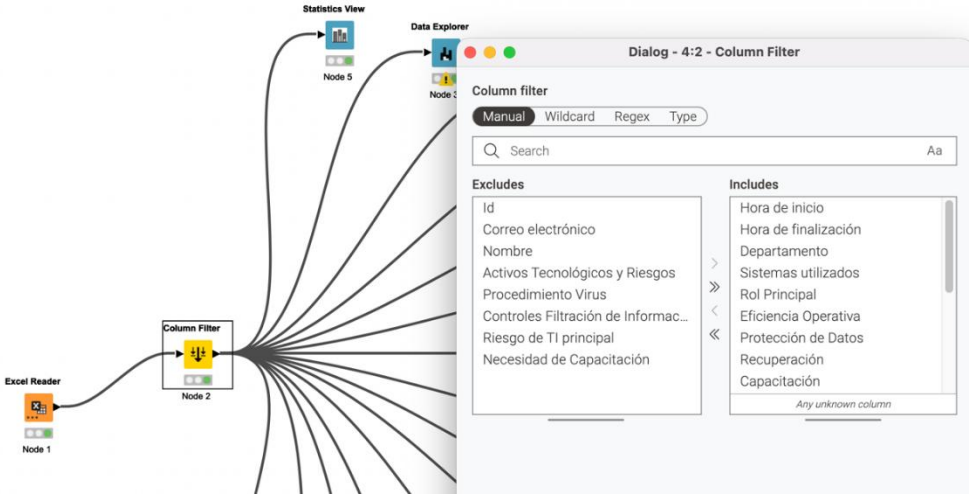


Figura 7: Aplicación de filtro de columnas en KNIME para datos provenientes de la encuesta.

Fuente: Elaboración propia.

Existen diferentes variables de tipo cuantitativo, sobre todo en la Sección 2 de la encuesta, por lo que se debe hacer un análisis exploratorio de estos datos para encontrar información que puede ser valiosa, como la que muestra la tabla 16; se hace notar que no tienen valora faltantes y exceptuando la variable Recuperación, todas tienen rangos diferentes de valores.

Tabla 16. Datos estadísticos de variables de tipo cuantitativo.

Datos estadísticos de la encuesta

Name	# Missing values	Minimum	Maximum	Mean	Standard Deviation	Sum	10 most common values
Eficiencia Operativa	0	2	5	4.615	0.87	60	5 (10; 76.92%), 4 (2; 15.38%), 2 (1; 7.69%)
Protección de Datos	0	4	5	4.846	0.376	63	5 (11; 84.62%), 4 (2; 15.38%)
Recuperación	0	5	5	5	0	65	5 (13; 100.0%)
Capacitación	0	3	5	4.769	0.599	62	5 (11; 84.62%), 3 (1; 7.69%), 4 (1; 7.69%)
Ransomware	0	3	5	4.769	0.599	62	5 (11; 84.62%), 3 (1; 7.69%), 4 (1; 7.69%)
Filtración de datos	0	4	5	4.846	0.376	63	5 (11; 84.62%), 4 (2; 15.38%)
Caída ERP	0	3	5	4.692	0.63	61	5 (10; 76.92%), 4 (2; 15.38%), 3 (1; 7.69%)
Error Humano	0	3	5	4.154	0.689	54	4 (7; 53.85%), 5 (4; 30.77%), 3 (2; 15.38%)
Incumplimiento Regulatorio	0	4	5	4.846	0.376	63	5 (11; 84.62%), 4 (2; 15.38%)

Fuente: Elaboración propia.

De igual manera, se realizó un análisis estadístico de las variables de tipo cualitativo y solamente la variable Manejo Incidente posee valores faltantes, lo cual se puede explicar gracias a que es una pregunta dependiente de la respuesta de otra, en este caso de la variable Experiencia en Incidentes.

Tabla 17: Datos estadísticos de variables de tipo nominal.

Column	No. missings	Unique values	All nominal values	Frequency Bar Chart
Departamento	0	5	Administración y Finanzas, Visitas Médicas, Comercial, Regencia y Calidad, Formación Médica	
Sistemas utilizados	0	7	Plataforma de correo electrónico (Outlook, Gmail);Herramientas de oficina (Suite de Microsoft Office);, ERP (Sistema de Planificación de Recursos Empresariales, como ser Microsoft Dynamics);Plataforma de correo electrónico (Outlook, Gmail);Herramientas de oficina (Suite de Microsoft Office);, Plataforma de correo electrónico (Outlook, Gmail);, ERP (Sistema de Planificación de Recursos Empresariales, como ser Microsoft Dynamics);Plataforma de correo electrónico (Outlook, Gmail);, Plataforma de correo electrónico (Outlook, Gmail);Herramientas de oficina (Suite de Microsoft Office);ERP (Sistema de Planificación de Recursos Empresariales, como ser Microsoft Dynamics);, Plataforma de correo electrónico (Outlook, Gmail);Close Up Analyzer, Power BI;, Herramientas de oficina (Suite de Microsoft Office);Plataforma de correo electrónico (Outlook, Gmail);	
Rol Principal	0	3	Liderazgo / Supervisión (tengo personal a mi cargo), Colaborador Técnico / Especializado (mi rol requiere conocimientos técnicos específicos), Colaborador Administrativo / Soporte (mi rol se centra en tareas administrativas y de soporte)	
Formación en Ciberseguridad	0	4	Sí, pero hace mucho tiempo, No, nunca., No estoy seguro/a., Sí, de forma regular y actualizada.	
Experiencia en Incidentes	0	2	No, nunca., Sí, en una ocasión.	
Manejo Incidente	9	2	Reporté inmediatamente al departamento de TI., No supe qué hacer / No lo reporté.	
Frecuencia Backup	0	5	Solo cuando me lo indican, Nunca / No sé cómo hacerlo, Diariamente, Mensualmente, Semanalmente	

Fuente: Elaboración propia.

4.1.2 LIMPIEZA Y PREPARACIÓN DE LOS DATOS

- Reporte de Tickets

Descrito en la figura 7, para evitar utilizar columnas o variables que no fueran necesarias para el estudio de los datos del reporte de tickets, se aplicó un filtro de columnas dentro de KNIME; de igual manera, teniendo en cuenta que el único valor numérico de este set de datos es **Tiempo Respuesta**, es necesario que este sea estudiado en su comportamiento para saber qué métodos de limpieza se deben aplicar y así mantener una homogeneidad en los datos.

El nodo **Numeric Outliers** nos permite visualizar y tratar los datos que se consideren anomalías, en este caso significando que fueron tickets que tomaron un mayor tiempo de respuesta de lo normal, para lo cual en el procesamiento se tomará la opción de remover estas filas.

Posteriormente a configurar el nodo, KNIME automáticamente crea una pequeña tabla en donde muestra los datos más importantes del estudio de valores atípicos, que también, para hacer una vista mejor presentable, se utilizará el nodo **Vista de Tabla.**

El resultado es que Tiempo Resolución posee **21 valores atípicos**, lo que representa un **8.5%** de los datos aproximadamente; si bien el límite inferior se muestra negativo, en -545.373, esto **no** es posible, debido a que se está midiendo una variable de tiempo, por lo cual se considerará que el *Límite Inferior* de *Tiempo Resolución* es **0**, así mismo, como el *Límite Superior* es **1,079.893**

horas, se considera que cualquier valor mayor que este es estadísticamente atípico.

Tabla 18. Resultado de valores atípicos

Detección de valores atípicos

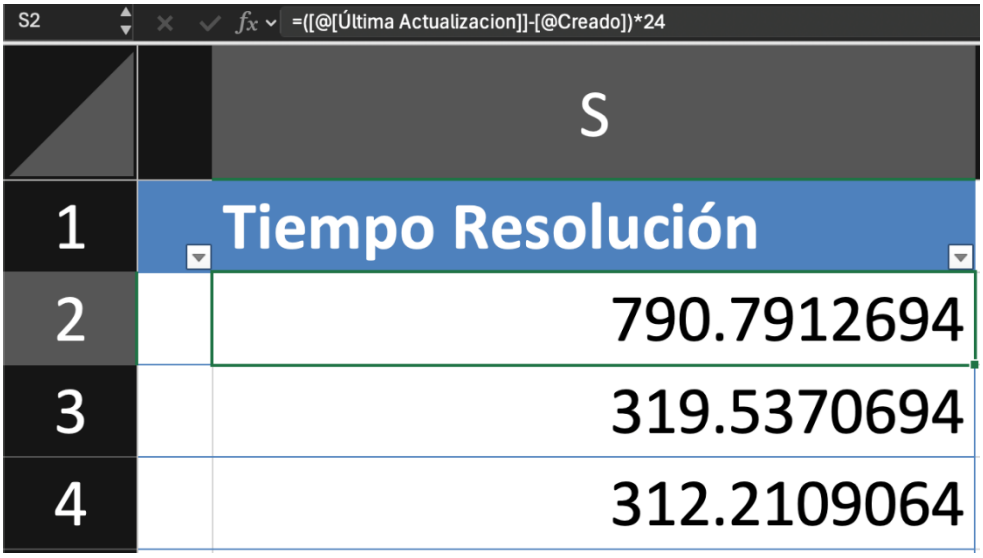
Outlier column *String*	Member count *Number (integer)*	Outlier count *Number (integer)*	Lower bound *Number (double)*	Upper bound *Number (double)*
Tiempo Resolución	248	21	-545.373	1,079.893

Fuente: Elaboración propia

El set de datos no tiene valores faltantes, por lo que en ese aspecto no fue necesario utilizar otros métodos de limpieza o llenados orientados a esta problemática.

La columna Tiempo Respuesta fue creada en base al resultado de la diferencia entre la fecha de creación del ticket, que corresponde a la variable **Creado** y la fecha de la última actualización, que, considerando que todos los tickets incluidos en este reporte ya están finalizados, es la variable que cuenta como la finalización del ticket. Ver Tabla 19.

Tabla 19. Columna emergente "Tiempo de Resolución"



Fuente: Elaboración propia.

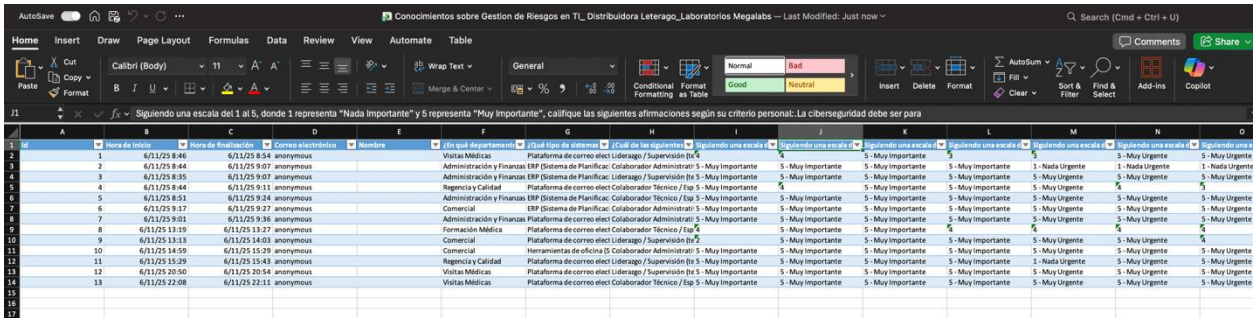
- Respuestas de encuesta estructurada

Para poder procesar los resultados de la encuesta dentro de la herramienta Knime, fue necesario primero hacer ciertos cambios al archivo de Excel para asegurar la integridad y el procesamiento correcto del archivo.

Reflejando en la tabla 20, donde se muestra el archivo de Excel sin modificar, las columnas

no tienen el mismo nombre planteado en el diccionario de datos, por lo cual se debe modificar primero para poder realizar el estudio correcto.

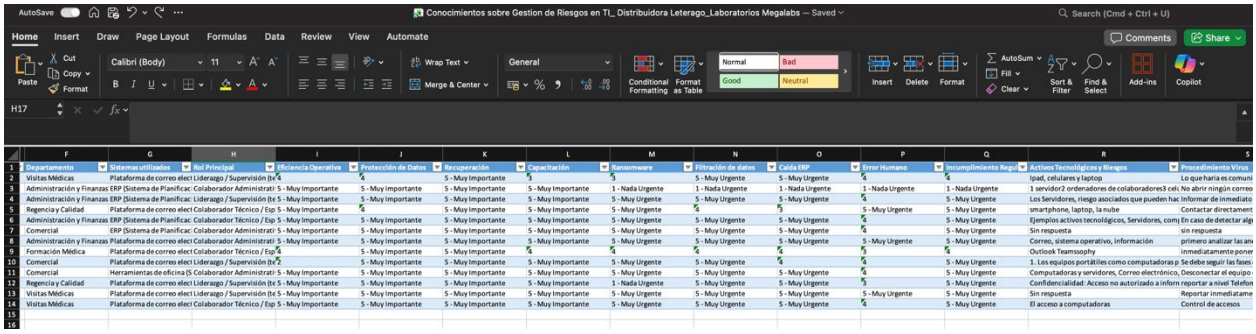
Tabla 20. Resultados de encuesta – Datos Generales



Fuente: Elaboración propia

Una vez modificadas las columnas, es necesario identificar que las respuestas en las variables de tipo cuantitativo, o sea, las que pertenecen a la Sección 2 mostrada en el diccionario de datos, no vienen directamente con el número, sino acompañadas de un texto a la derecha (Muy Urgente o Muy Importante, dependiendo de la pregunta), por lo cual es necesario aplicar funciones de reemplazo de texto para que estos puedan ser procesados correctamente en KNIME; ver tablas 21 y tabla 22 para notar el cambio que tienen las columnas.

Tabla 21. Resultados de encuesta con nombres de columnas modificados



Fuente: Elaboración propia

Tabla 22. Resultados de encuesta con reemplazo de texto para mantener variables cuantitativas

Fuente: Elaboración propia

4.1.3 VISUALIZACIÓN DE DATOS

- Reporte de Tickets

Se realizó un histograma para detectar la frecuencia total de los tiempos de respuesta, para

lo cual todos los datos se dividen entre las diferentes distribuciones, y se encontró que la mayoría de los datos están agrupados en el primer grupo, que corresponde de 0 a 500 horas, como se muestra en la siguiente gráfica.

163 registros se atendieron entre 0 a 500 horas, lo cual representa un 66% de los datos, mientras que la segunda frecuencia más alta es entre 500 a 1000 horas con 51 registros, lo que representa un **21% de los datos.**

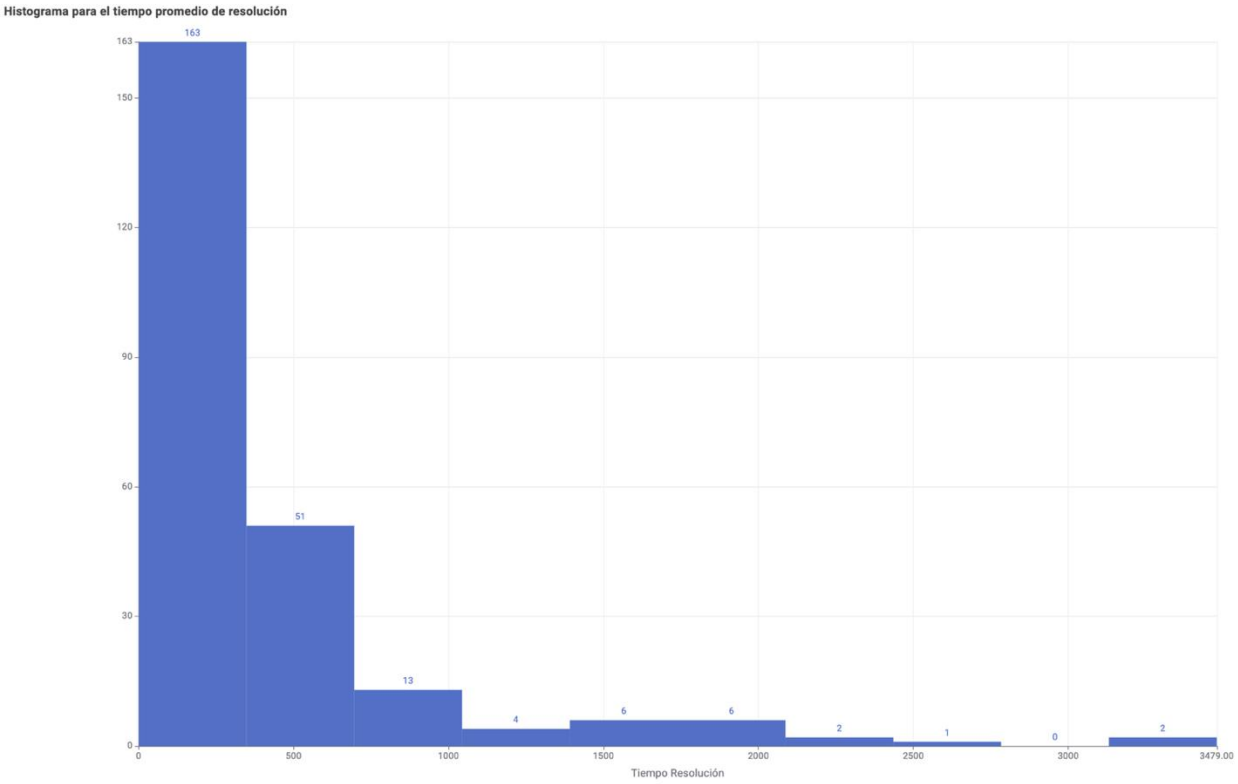


Figura 8. Histograma para el MTTR

Fuente: Elaboración propia.

El siguiente gráfico de barras retrata el tiempo de resolución promedio de un ticket en base

a la prioridad asignada, y, por el comportamiento de la gráfica, se puede decir que los tickets que se atienden de manera más rápida, o que tienen un menor tiempo de resolución son aquellos cuya prioridad es **Alta**, con un tiempo promedio de **346.34 horas**, mientras que cuando se le asigna prioridad baja, este tiempo tiene un mayor diferencia, con **1020.43 horas** en promedio, lo cual es una disparidad bastante alta, considerando la diferencia que existe entre prioridad Media y Urgente, con **407.94** y **396.37 horas**, respectivamente.

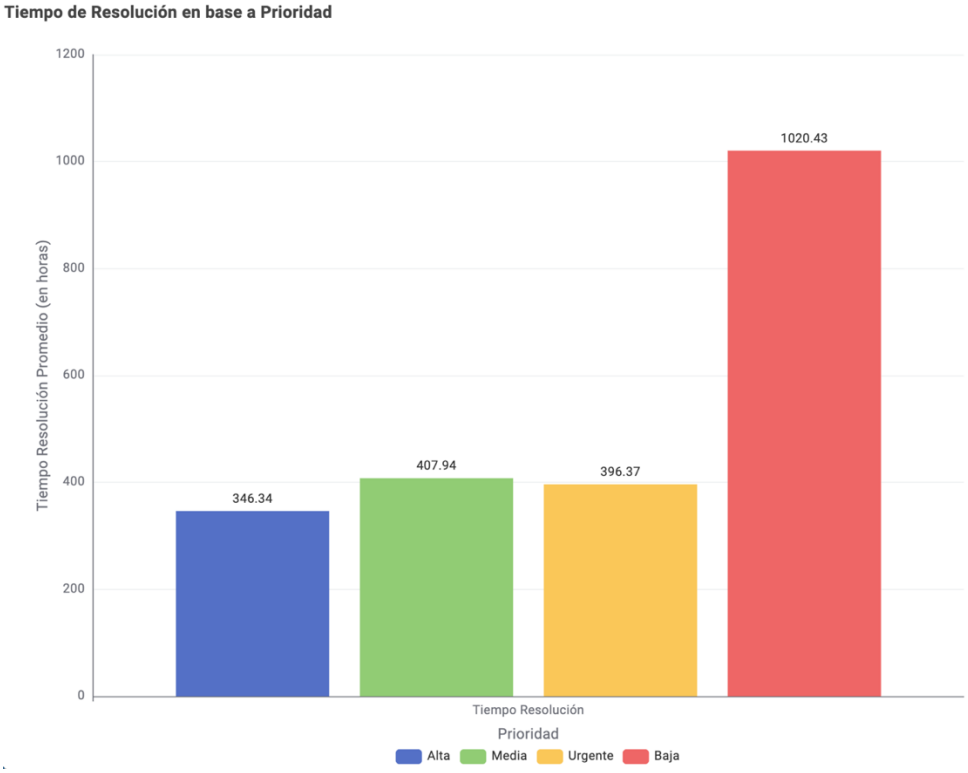


Figura 9. MTTR en base a la prioridad del ticket.

Fuente: Elaboración propia

El gráfico mostrado en la figura 10 corresponde al MTTR en base al servicio que la empresa ofrece a sus usuarios internos.

Es posible ver que hay una diferencia de tiempo de resolución marcada entre **AX Pharma 365**, que corresponde al ERP que la empresa utiliza, ante los demás servicios que se ofrecen. Teniendo un promedio de **103 horas** por ticket, solamente **Software Corporativo**, que posee **73 horas** en promedio, y situaciones con el Hardware Local/Equipamiento, que posee 30 horas en promedio, son los más próximos en la distribución, lo que significa que el mayor influjo de incidencias y solicitudes de apoyo provienen del ERP.

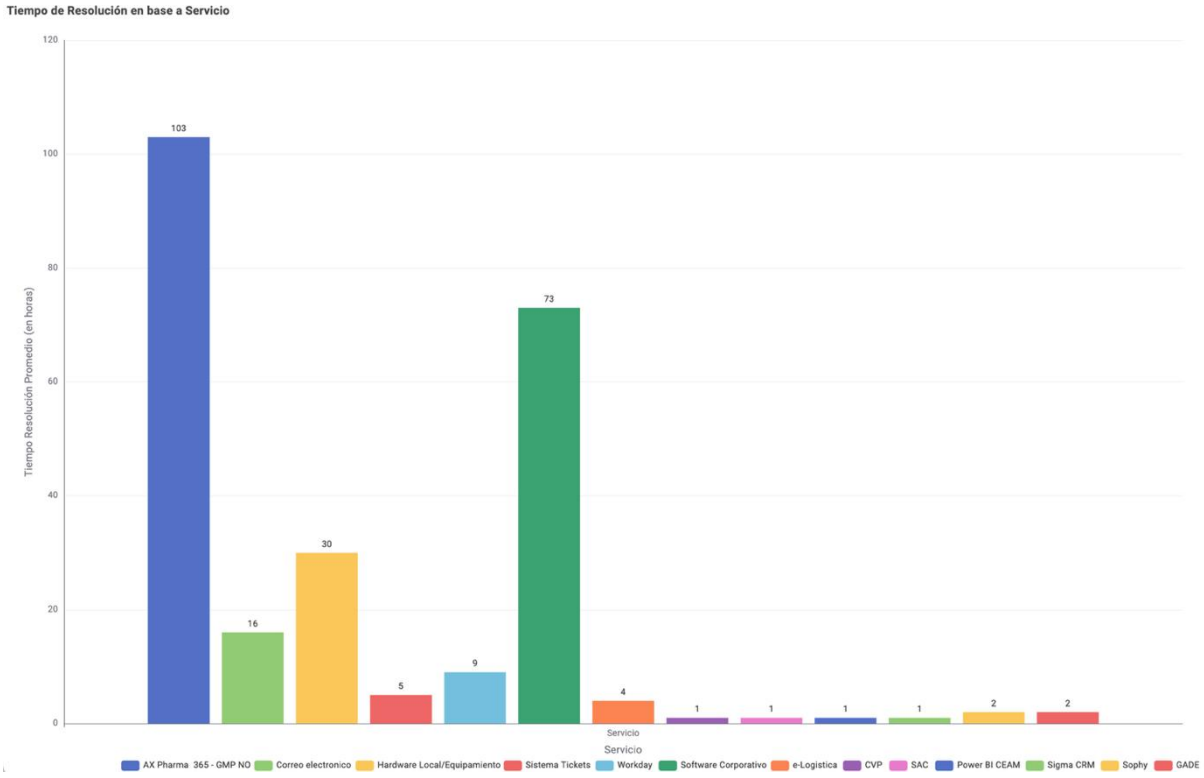


Figura 10. MTTR en base al Servicio del que se está solicitando asistencia.

Fuente: Elaboración propia.

La figura 11 muestra por medio de un gráfico de densidad la manera en la que el tiempo de resolución promedio está distribuido por departamento; de la misma manera en la que la figura 13 muestra que la mayoría de los tickets ronda en un rango entre 0 y 500 horas de resolución, este gráfico muestra también el departamento en donde más se concentran estas solicitudes realizadas en el sistema.

El área de Logística es quien más tiene un influjo de tickets que se solucionan alrededor de la primera mitad del intervalo de 0 a 500, seguido por otras áreas como Tecnología Informática, lo cual puede ser explicado como el ingreso de incidencias que afectan directamente al área de TI, seguido de Contabilidad, Regencia y Calidad y Gestión Humana, entre un máximo de 5 áreas.

Es necesario tener en cuenta, que si bien la mayoría de los tickets ronda en el primer intervalo de 0-500, el área de Gestión Humana posee un pico de densidad alta en el segundo

intervalo que va de 500 a 1000 horas como tiempo de resolución.

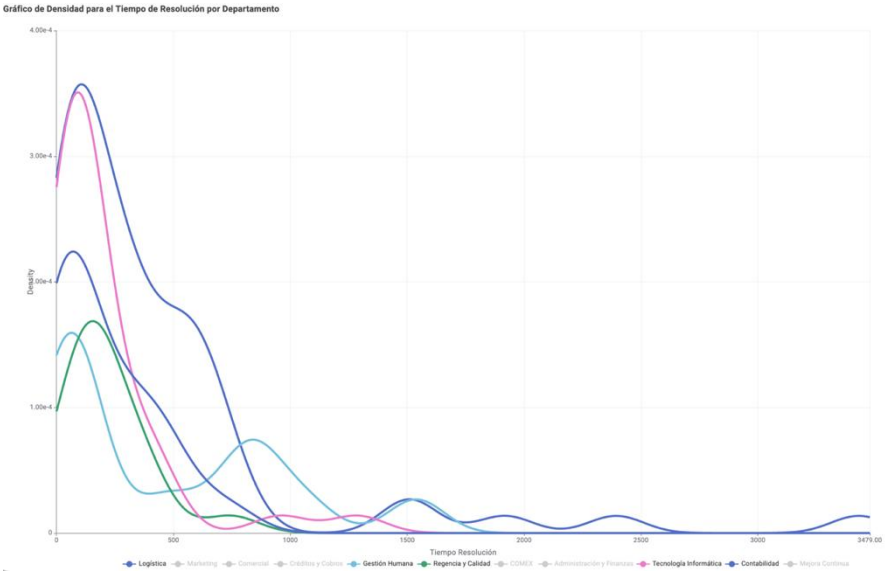


Figura 11. Densidad del MTTR por área

Fuente: Elaboración propia.

El gráfico que pertenece a la figura 12 hace referencia a la cantidad de tickets que se reciben por Departamento, dentro del cual el mayor solicitante es el área de Logística, los cuales poseen 58 tickets realizados, que corresponden a un 23.39% de todos los datos.

El área de Créditos y Cobros posee la cantidad más cercana a la que tiene Logística, con 39 tickets que representan un 15.73% de los datos, por lo cual se puede decir que el área de Logística es donde ocurren más incidencias que se necesitan atender.

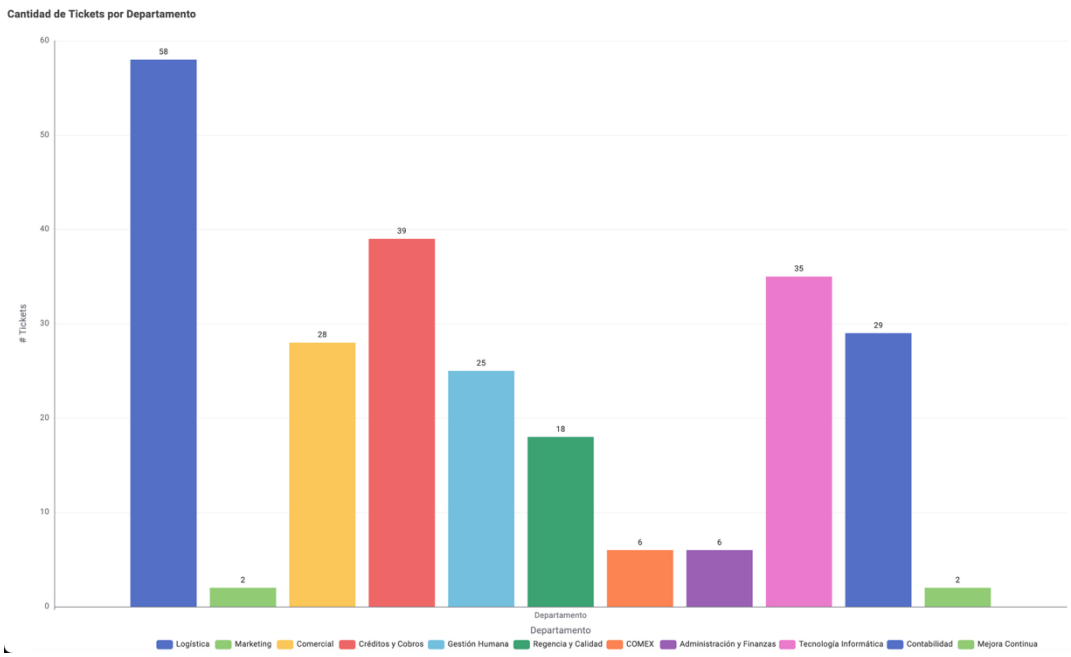


Figura 12. Cantidad de tickets por área

Fuente: Elaboración propia

La figura 13 muestra un gráfico de dispersión para la distribución de cada departamento sobre los tiempos de resolución promedio, lo cual hace validar la primera observación que se tenía sobre el gráfico de densidad, dónde se tiene en cuenta de que si bien el área de logística es quien tiene un mayor influjo de tickets también la mayoría de los tickets que están atendidos rondan entre el intervalo de 0 a 500 horas de trabajo realizado en promedio.

De igual manera, es posible validar la parte de valores atípicos para el tiempo de resolución en donde se puede ver que después del límite superior qué la herramienta KNIME había definido existen muy pocos datos y no representan un promedio de atención al usuario.

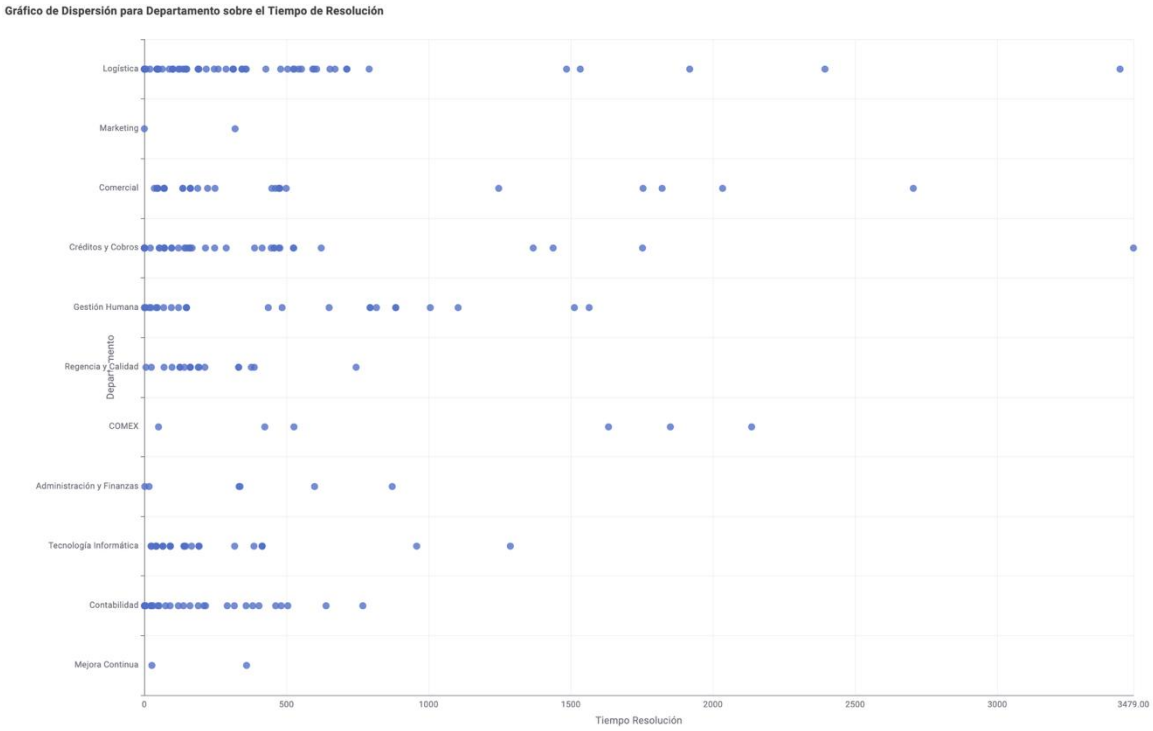


Figura 13. Puntos de dispersión en el MTTR por área

Fuente: Elaboración propia

- Resultados de encuesta estructurada

Para la figura 14, se toma en cuenta la distribución que hay de colaboradores por departamento, donde la mayoría de los que respondieron pertenecen al área de **Administración y Finanzas (4 personas),** seguidos del área **Comercial** y de **Visitas Médicas** (**3 personas**), y, por último, siendo la minoría dentro de esta muestra, la persona que pertenece al área de **Formación Médica (1 persona).**

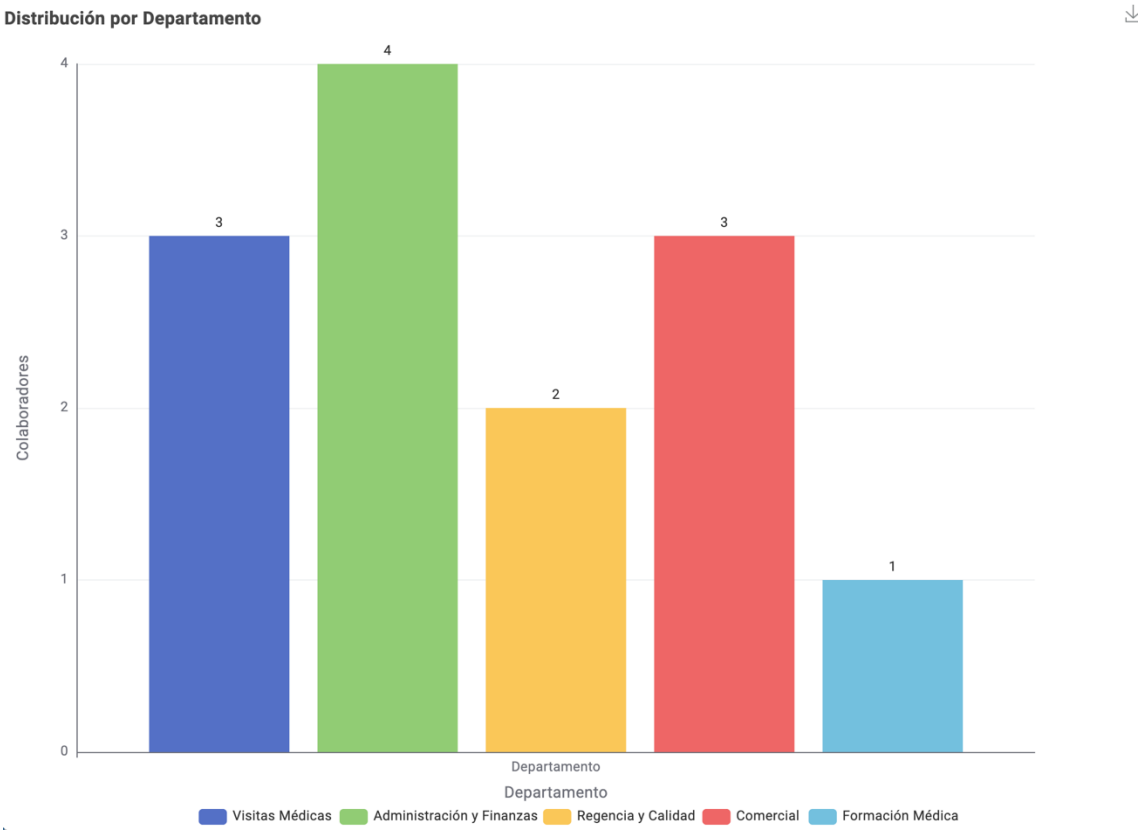


Figura 14. Distribución de encuestados por área

Fuente: Elaboración propia

La figura número 15 muestra la distribución de las personas que fueron encuestadas por el tipo de rol organizacional que tienen.

La mayoría de los que respondieron, en este caso, fueron **5 personas** que pertenecen a un rol de **Liderazgo o Supervisión,** el cual toma en cuenta que tiene personal a su cargo.

En el segundo puesto, ambos roles con la misma cantidad de personas (**4 personas**) pertenecen a colaboradores **Administrativos o Soporte**, y **Colaboradores**

Técnicos/Especializados.

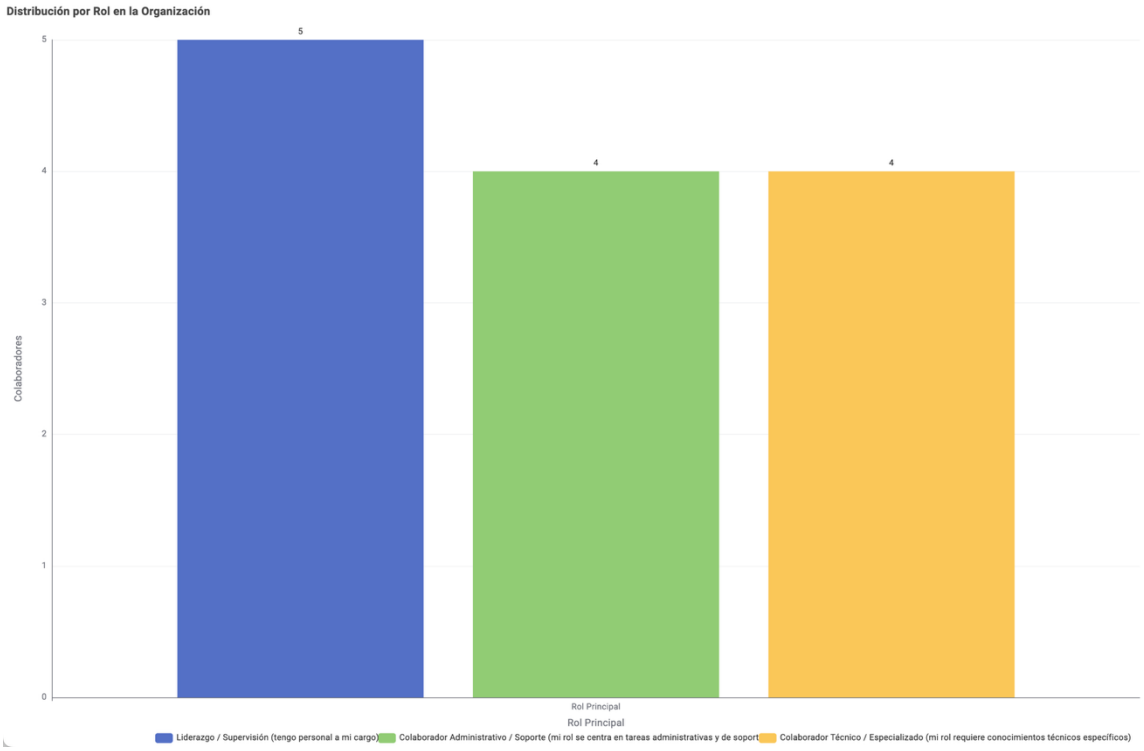


Figura 15. Distribución de encuestados por rol organizacional

Fuente: Elaboración propia

La figura número 16 muestra la pregunta que se le hizo a la muestra sobre si se había recibido formación de cómo detectar amenazas de ciberseguridad; en un entorno tecnológico tan avanzado y tan de rápido movimiento como el que existe hoy en día, la gran mayoría, en este caso **6 personas que corresponden al 46.15% de las personas encuestadas**, retratan que **sí** han recibido formación sobre cómo detectar amenazas de ciberseguridad, pero que fue hace *mucho tiempo*, lo cual indica que puede existir un **desfase o desactualización** en el conocimiento que se tiene sobre la prevención de incidentes en el entorno tecnológico.

Mientras **3 personas** han respondido que **nunca** han recibido formación sobre cómo detectar amenazas de ciberseguridad, por último, en la misma categoría se encuentra el *"No estoy seguro",* que son **2 personas** y *"sí, de forma regular y actualizada",* también siendo **2 personas**.

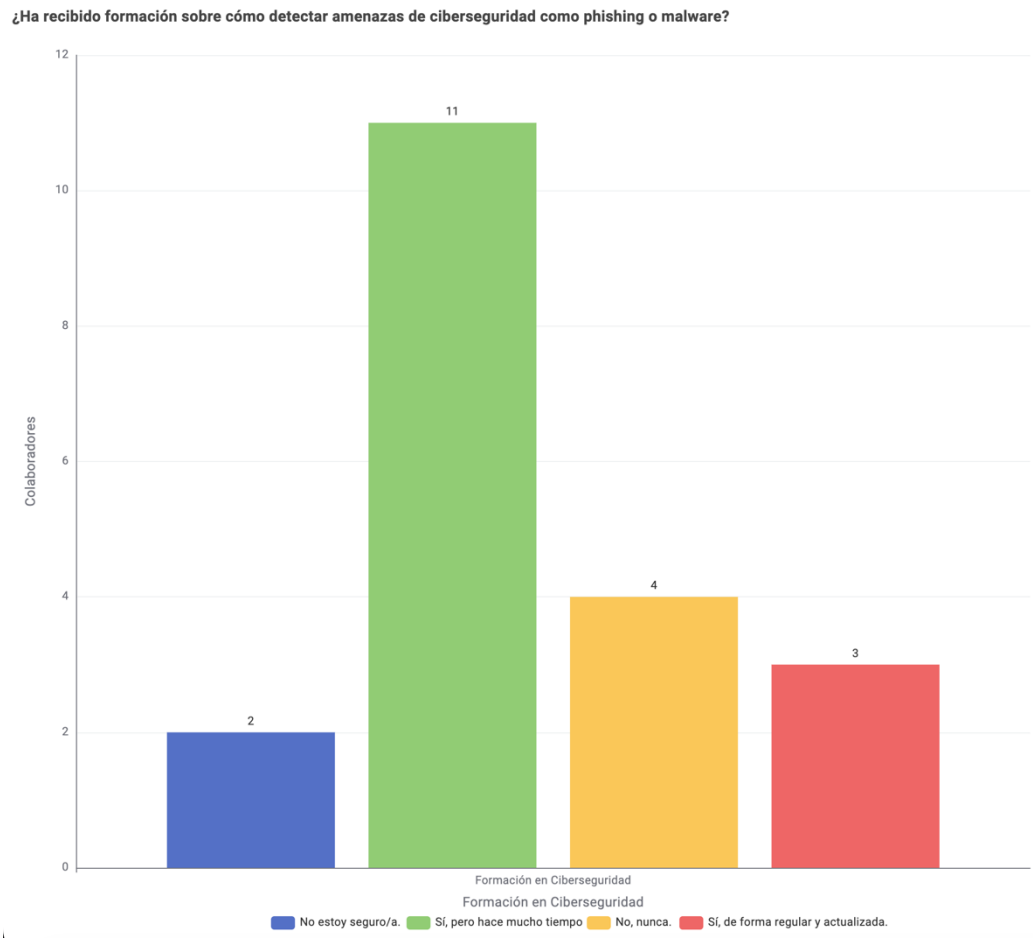


Figura 16. Formación sobre detección de phishing o malware, en los encuestados

Fuente: Elaboración Propia

Para la figura 17 se muestra un gráfico que mide el nivel de importancia que consideran los encuestados sobre la eficiencia operativa y cómo ésta se relaciona con los procesos del área de TI, como ser la gestión y la seguridad de la información.

Las personas que pertenecen al área de Administración y Finanzas y Regencia y Calidad consideran que sí es de suma importancia la parte de gestión y seguridad de la información para que afecte de manera positiva al área de TI. Se debe tener en cuenta que el área Comercial, de Formación Médica y el área de Visitas Médicas si bien no tienen ingresado como muy importante o un nivel 5 (ya que califican de 4 a 4.67) siempre consideran la eficiencia operativa importante dentro de sus áreas y cómo ésta se relaciona con la gestión de activos del área de TI puede ser un poco menos importante que otras funciones que tenga asignadas.

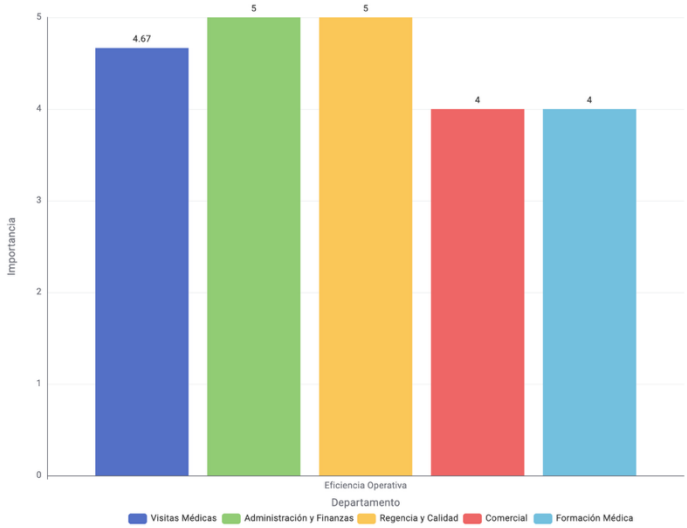


Figura 17. Nivel de importancia considerada por los encuestados sobre la eficiencia operativa

Fuente: Elaboración Propia

La figura 18 muestra el nivel de importancia que consideran los encuestados sobre la protección de datos, dentro de la cual el resultado es casi unánime, llegando casi al **5** que significa **muy importante**.

El área de **Administración y Finanzas, el Área Comercial y el área de Formación Médica** consideran que la protección de datos es muy importante dentro de los planes de gestión de riesgos y gestión de activos de TI.

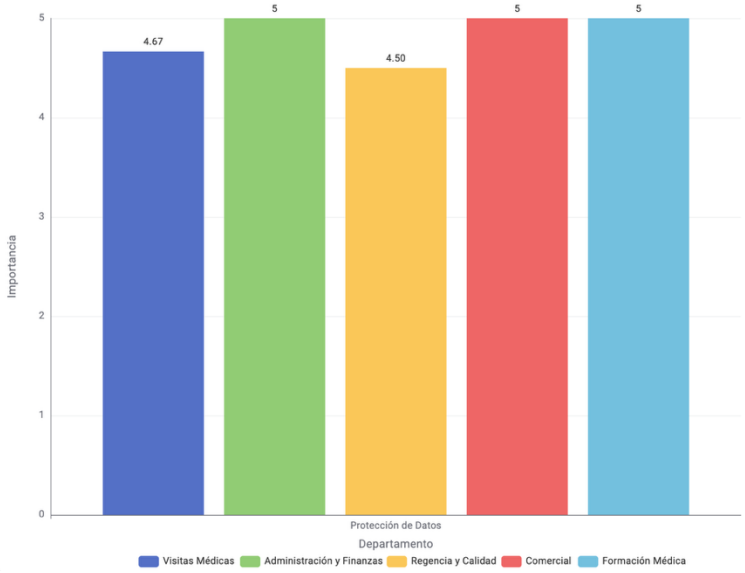


Figura 18. Nivel de importancia considerada por los encuestados sobre la protección de datos

Fuente: Elaboración Propia

De acuerdo con la figura 19, el gráfico que muestra el nivel de importancia que consideran los encuestados sobre contar con un plan de recuperación de TI es de manera unánime muy importante, con un valor de **5.**

Todas las áreas encuestadas concuerdan que esto debe ser lo más importante para que un plan d**e gestión** sea lo más claro y eficiente posible.

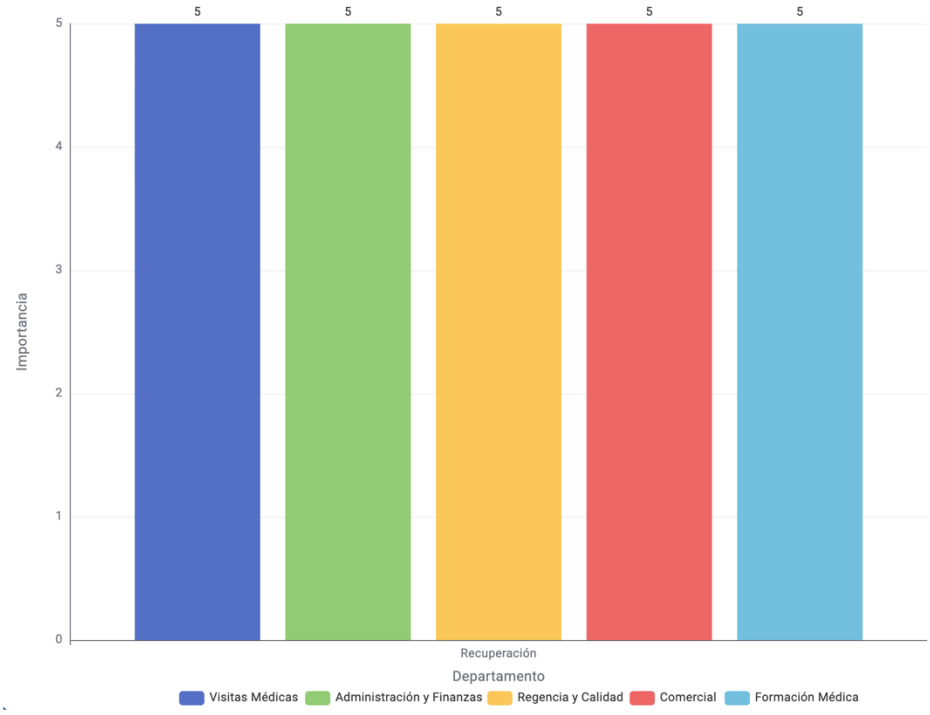


Figura 19. Nivel de importancia considerada por los encuestados acerca de contar con un plan de recuperación de TI

Fuente: Elaboración Propia

La figura 20 muestra el nivel de importancia que consideran los encuestados sobre recibir capacitaciones constantes en temas de ciberseguridad con el propósito de mantener un conocimiento sobre la gestión de TI y sus activos, para lo cual 3 áreas (***Administración y Finanzas, Regencia y Calidad, Área Comercial)*** consideran que es muy importante (**puntuación de 5**). En cambio, el área de visitas médicas y el área de formación médica consideran que es menos

importante que otros asuntos, con un **puntaje promedio de 4.33 y 4**, respectivamente.

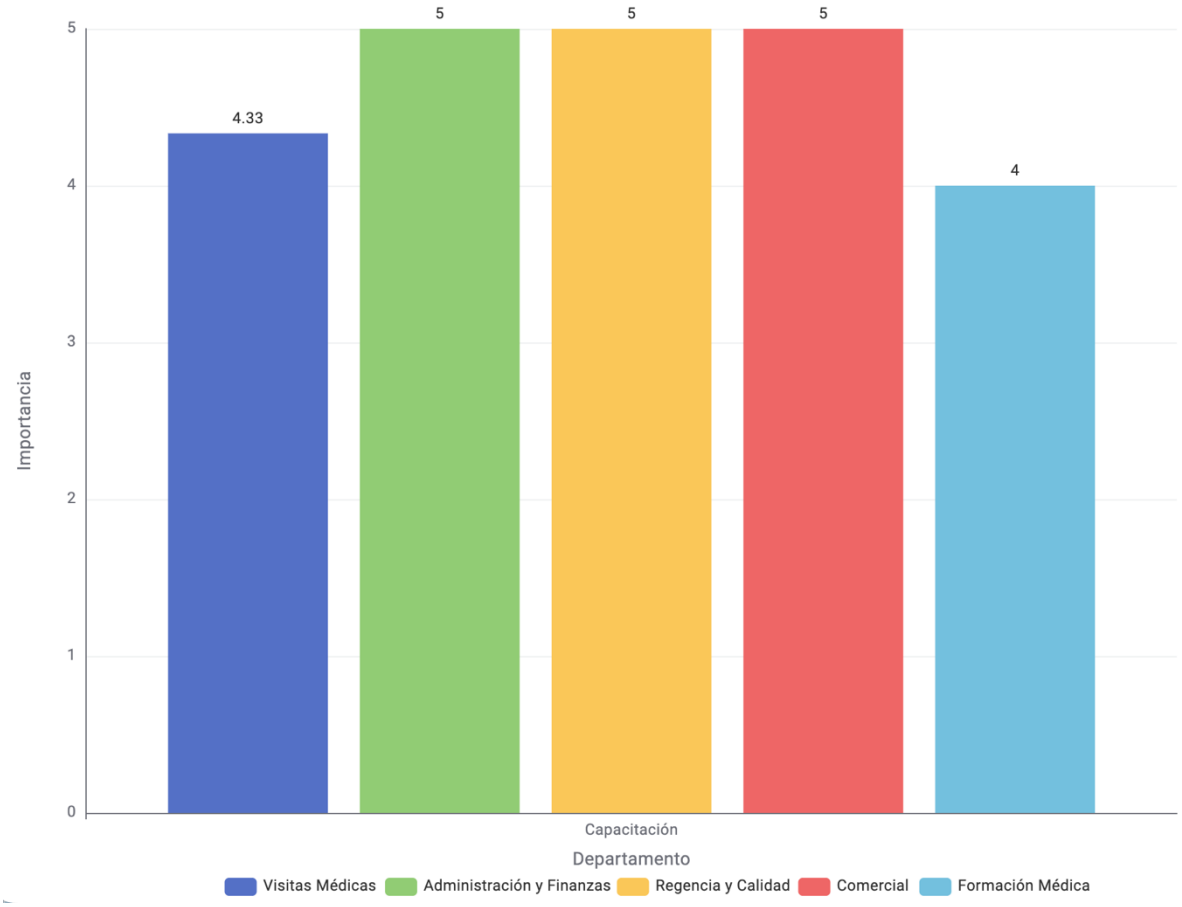


Figura 20. Nivel de importancia considerada por los encuestados sobre la capacitación constante en temas de ciberseguridad

Fuente: Elaboración Propia

La figura 21 muestra el nivel de urgencia que consideran los encuestados sobre un ataque posible de ransomware, para lo cual las áreas de **Administración y Finanzas, Regencia y Calidad, y el área Comercial** consideran que es muy urgente **(puntuación de 5)**.

En cambio, el área de **Formación Médica** y el área de **Visitas Médicas** consideran que tiene una menor gravedad, con **puntajes promedio de 4 y 4.33**, respectivamente.

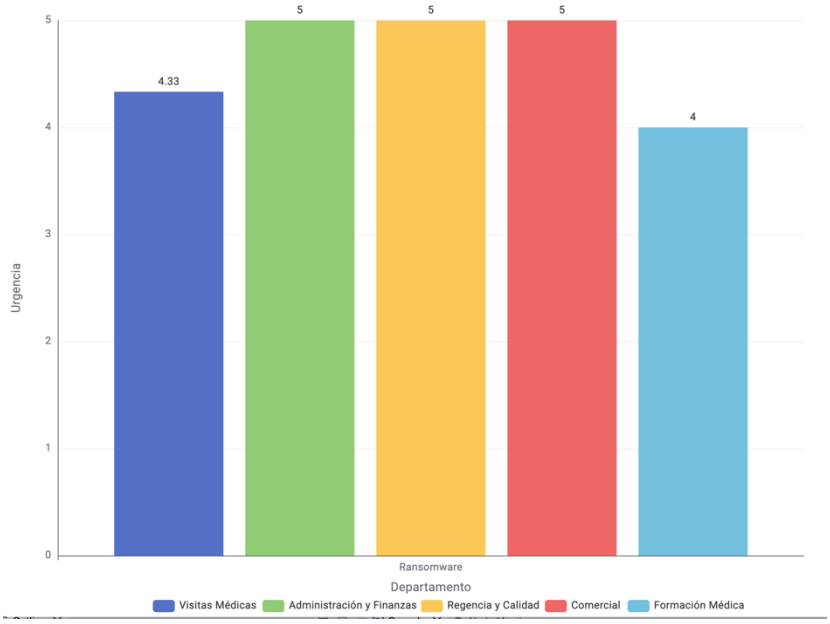


Figura 21. Nivel de urgencia considerada por los encuestados sobre un ataque de ransomware
Fuente: Elaboración Propia

La figura 22 muestra el nivel de urgencia que consideran los encuestados sobre un suceso posible de filtración de datos, para lo cual la mayoría de las áreas responden que tiene un nivel mayor de urgencia **(puntuación de 5),** sin embargo, el área de **Regencia y Calidad** y el área de **Formación Médica** lo tienen con una estima menor que el área de **Visitas Médicas y Administración y Finanzas**, **siendo de 4.50 y 4,** respectivamente.

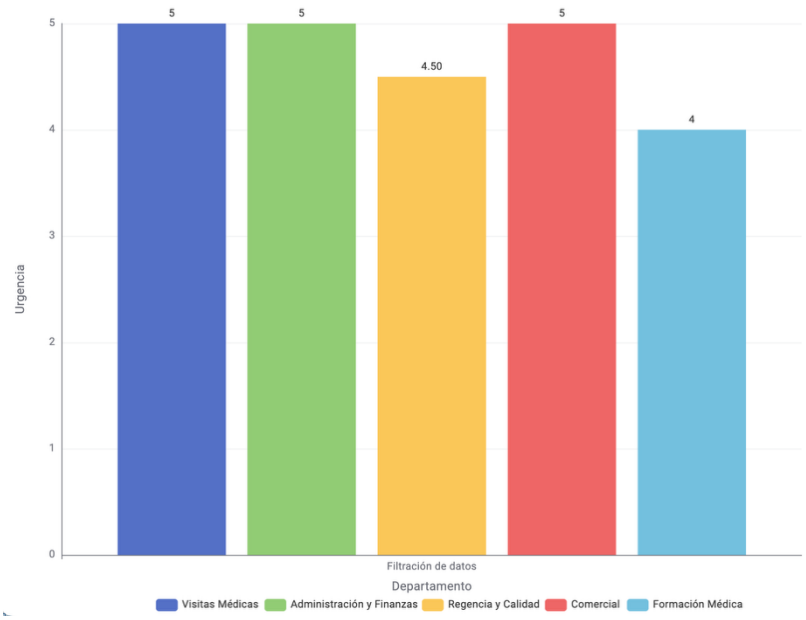


Figura 22. Nivel de urgencia considerada por los encuestados sobre un suceso de filtración de datos

Fuente: Elaboración Propia

La figura 23 muestra el nivel de urgencia que consideran los encuestados sobre un suceso que no les permita acceder al ERP que maneja la empresa, para lo cual el área de **Administración y Finanzas** y el área de **Visitas Médicas** consideran que tiene una urgencia mucho mayor (**puntuación de 5**) que como lo considerarían el área de **Regencia y Calidad**, área **Comercial** y el área de **Formación Médica**, con puntuaciones de **4, 4.67 y 4, respectivamente**.

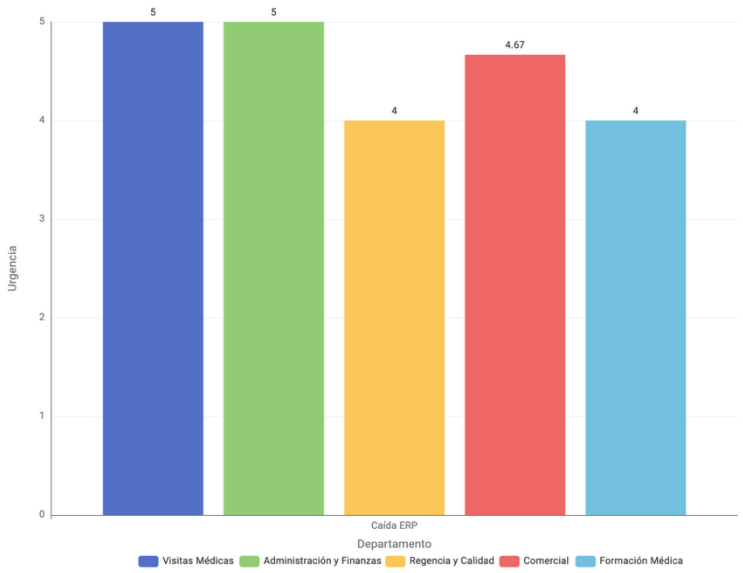


Figura 23. Nivel de urgencia considerada por los encuestados sobre una inaccesibilidad al ERP

Fuente: Elaboración Propia

La figura 24 muestra el nivel de urgencia que se considera sobre el error humano en los procesos tecnológicos, plasmado con el ejemplo de un correo enviado a un destinatario equivocado, para lo cual la mayoría de los encuestados encontró que tiene un nivel de urgencia mayor a lo moderado (***puntuación de 4 o mayor a 4***), teniendo en cuenta las respuestas de personas que pertenecen al área de **Administración y Finanzas**, fluctúan entre muy urgente a menos urgente. Quiénes poseen una percepción de menor urgencia sobre el error humano son las personas que pertenecían al área de **Formación Médica**, con una **puntuación de 3**.

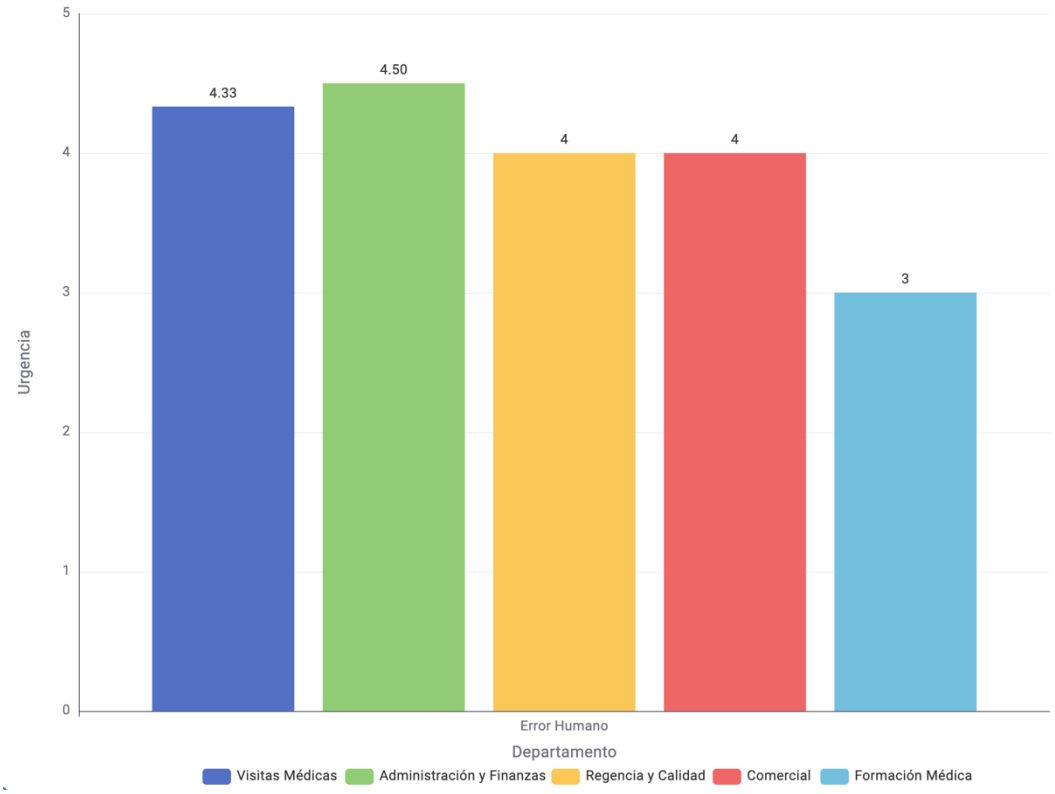


Figura 24. Nivel de urgencia considerada por los encuestados sobre el error humano en los procesos tecnológicos.

Fuente: Elaboración Propia

La figura 25 refleja el nivel de urgencia que consideran los empleados sobre el incumplimiento de regulaciones farmacéuticas, para lo cual 3 de las áreas que existen dentro del universo recolectado de datos responden que es de manera muy urgente (**Administración y Finanzas, Regencia y Calidad y Comercial**), con puntuaciones de **5**, mientras que el área de **Visitas Médicas** y **Formación Médica** lo consideran un poco menor de urgencia, con puntuaciones de **4.67 y 4,** respectivamente.

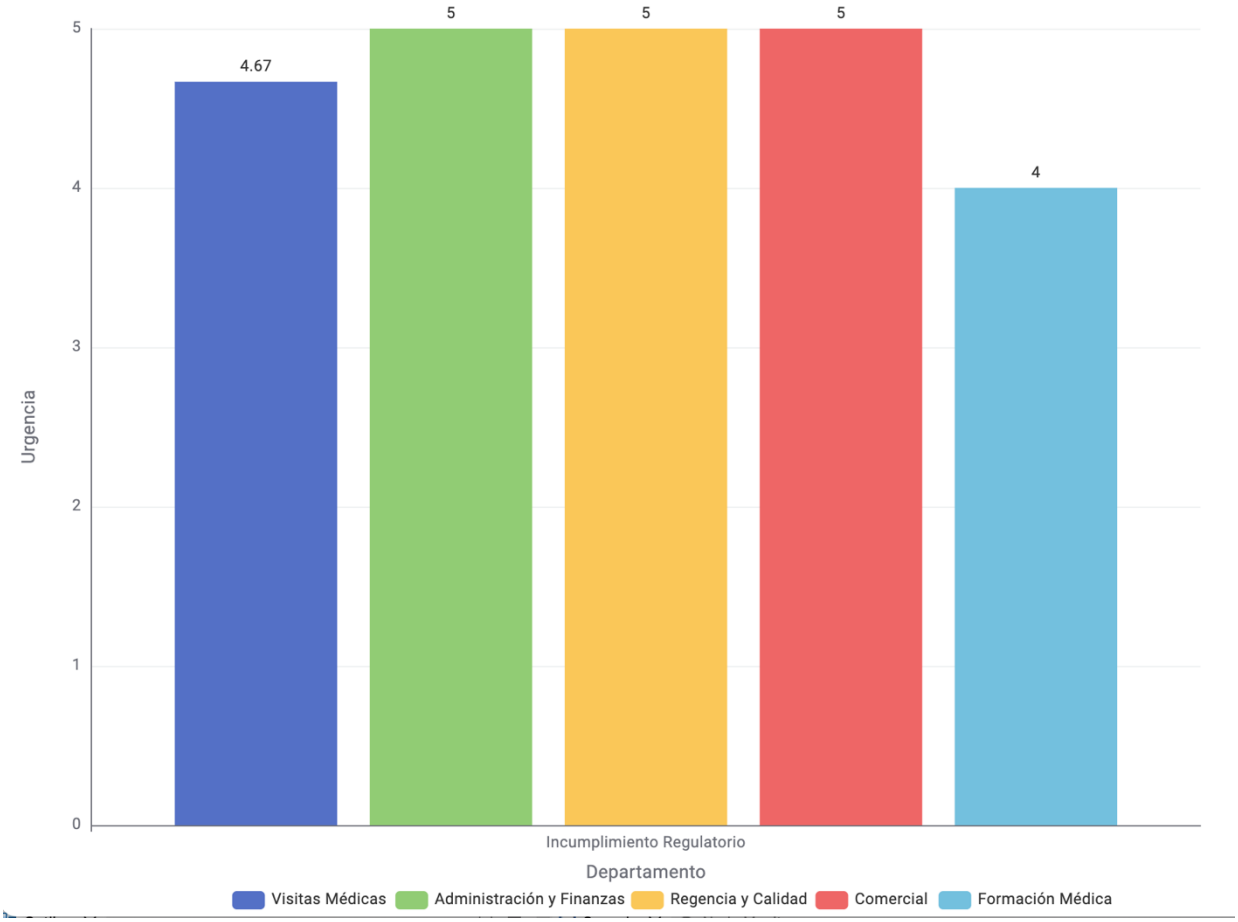


Figura 25. Nivel de urgencia considerada por los encuestados sobre el incumplimiento de regulaciones farmacéuticas.

Fuente: Elaboración Propia

4.2 INFORME DEL PROCESO DE RECOLECCIÓN DE DATOS

- Reporte de Tickets

De la misma manera en la que se ha planteado en las secciones anteriores, el reporte de Tickets proviene de un software llamado **Tickets**, el cual se utiliza dentro de la empresa para poder gestionar todos los casos, solicitudes o requerimientos de apoyo que se necesite por parte del área de Tecnologías de la Información.

Tomando en cuenta que el sistema posee una funcionalidad de reportería, esta reportería es descargable, con la diferencia qué se debe poner un intervalo de fechas definido para poder obtener

todos los resultados de ese tiempo en específico punto y seguido el equipo de investigadores tomó en cuenta el intervalo entre se septiembre de 2024 a septiembre de 2025

Luego de descargarlo directamente desde el sistema se recibe un archivo de tipo Excel, el cual luego fue tratado y limpiado; se le creó una columna nueva (el campo Tiempo Respuesta) para poder cumplir todos los objetos de estudio.

Una vez que se hace el trabajo del formateo de la creación de nuevas columnas o del tratamiento de columna faltantes se puede ingresar a la herramienta KNIME, la cual funciona como un flujo de trabajo en donde se agregar diferentes elementos configurables que hacen estudios estadísticos a nivel de millones.

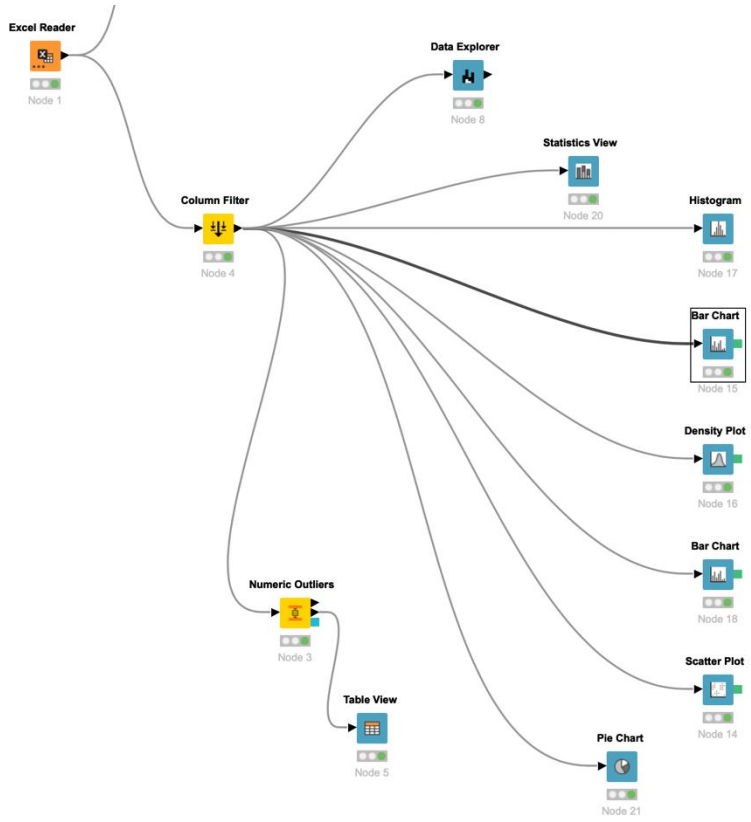
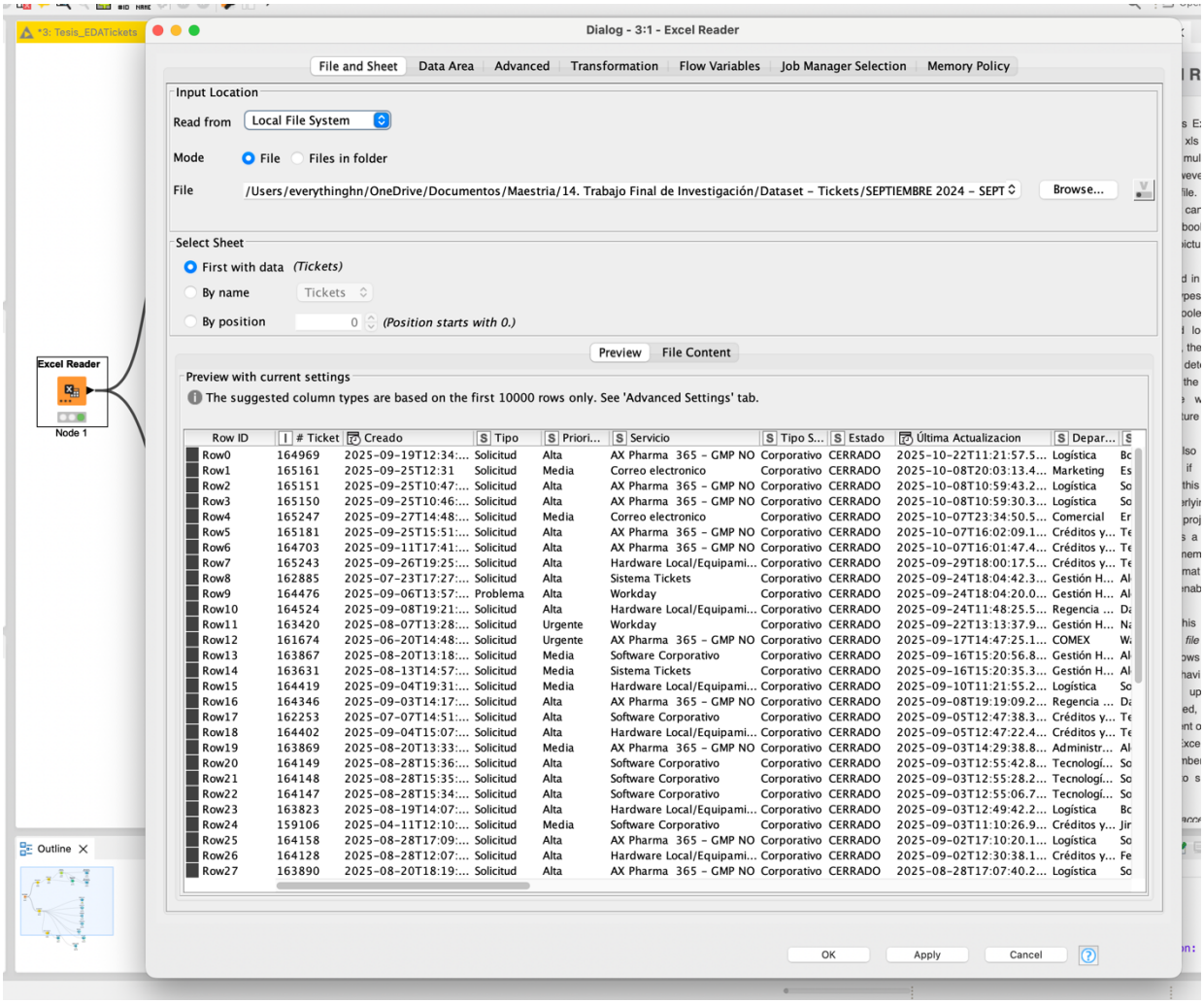


Figura 26. Esquema general para el análisis de datos del sistema de tickets en KNIME

Fuente: Elaboración Propia

La figura 27 muestra la inicialización del lector de Excel, y como se ven los datos en otro

lugar.



Row ID	# Ticket	Creado	Tipo	Priori...	Servicio	Tipo S...	Estado	Última Actualizacion	Depar...
Row0	164969	2025-09-19T12:34:...	Solicitud	Alta	AX Pharma 365 - GMP NO	Corporativo	CERRADO	2025-10-22T11:21:57.5...	Logística
Row1	165161	2025-09-25T12:31	Solicitud	Media	Correo electronico	Corporativo	CERRADO	2025-10-08T20:03:13.4...	Marketing
Row2	165151	2025-09-25T10:47:...	Solicitud	Alta	AX Pharma 365 - GMP NO	Corporativo	CERRADO	2025-10-08T10:59:43.2...	Logística
Row3	165150	2025-09-25T10:46:...	Solicitud	Alta	AX Pharma 365 - GMP NO	Corporativo	CERRADO	2025-10-08T10:59:30.3...	Logística
Row4	165247	2025-09-27T14:48:...	Solicitud	Media	Correo electronico	Corporativo	CERRADO	2025-10-07T23:34:50.5...	Comercial
Row5	165181	2025-09-25T15:51:...	Solicitud	Alta	AX Pharma 365 - GMP NO	Corporativo	CERRADO	2025-10-07T16:02:09.1...	Créditos y...
Row6	164703	2025-09-11T17:41:...	Solicitud	Alta	AX Pharma 365 - GMP NO	Corporativo	CERRADO	2025-10-07T16:01:47.4...	Créditos y...
Row7	165243	2025-09-26T19:25:...	Solicitud	Alta	Hardware Local/Equipami...	Corporativo	CERRADO	2025-09-29T18:00:17.5...	Créditos y...
Row8	162885	2025-07-23T17:27:...	Solicitud	Alta	Sistema Tickets	Corporativo	CERRADO	2025-09-24T18:04:42.3...	Gestión H...
Row9	164476	2025-09-06T13:57:...	Problema	Alta	Workday	Corporativo	CERRADO	2025-09-24T18:04:20.0...	Gestión H...
Row10	164524	2025-09-08T19:21:...	Solicitud	Alta	Hardware Local/Equipami...	Corporativo	CERRADO	2025-09-24T11:48:25.5...	Regencia ...
Row11	163420	2025-08-07T13:28:...	Solicitud	Urgente	Workday	Corporativo	CERRADO	2025-09-22T13:13:37.9...	Gestión H...
Row12	161674	2025-06-20T14:48:...	Solicitud	Urgente	AX Pharma 365 - GMP NO	Corporativo	CERRADO	2025-09-17T14:47:25.1...	COMEX
Row13	163867	2025-08-20T13:18:...	Solicitud	Media	Software Corporativo	Corporativo	CERRADO	2025-09-16T15:20:56.8...	Gestión H...
Row14	163631	2025-08-13T14:57:...	Solicitud	Media	Sistema Tickets	Corporativo	CERRADO	2025-09-16T15:20:35.3...	Gestión H...
Row15	164419	2025-09-04T19:31:...	Solicitud	Media	Hardware Local/Equipami...	Corporativo	CERRADO	2025-09-10T11:21:55.2...	Logística
Row16	164346	2025-09-03T14:17:...	Solicitud	Alta	AX Pharma 365 - GMP NO	Corporativo	CERRADO	2025-09-08T19:19:09.2...	Regencia ...
Row17	162253	2025-07-07T14:51:...	Solicitud	Alta	Software Corporativo	Corporativo	CERRADO	2025-09-05T12:47:38.3...	Créditos y...
Row18	164402	2025-09-04T15:07:...	Solicitud	Alta	Hardware Local/Equipami...	Corporativo	CERRADO	2025-09-05T12:47:22.4...	Créditos y...
Row19	163869	2025-08-20T13:33:...	Solicitud	Media	AX Pharma 365 - GMP NO	Corporativo	CERRADO	2025-09-03T14:29:38.8...	Administr...
Row20	164149	2025-08-28T15:36:...	Solicitud	Alta	Software Corporativo	Corporativo	CERRADO	2025-09-03T12:55:42.8...	Tecnologí...
Row21	164148	2025-08-28T15:35:...	Solicitud	Alta	Software Corporativo	Corporativo	CERRADO	2025-09-03T12:55:28.2...	Tecnologí...
Row22	164147	2025-08-28T15:34:...	Solicitud	Alta	Software Corporativo	Corporativo	CERRADO	2025-09-03T12:55:06.7...	Tecnologí...
Row23	163823	2025-08-19T14:07:...	Solicitud	Alta	Hardware Local/Equipami...	Corporativo	CERRADO	2025-09-03T12:49:42.2...	Logística
Row24	159106	2025-04-11T12:10:...	Solicitud	Media	Software Corporativo	Corporativo	CERRADO	2025-09-03T11:10:26.9...	Créditos y...
Row25	164158	2025-08-28T17:09:...	Solicitud	Alta	AX Pharma 365 - GMP NO	Corporativo	CERRADO	2025-09-02T17:10:20.1...	Logística
Row26	164128	2025-08-28T12:07:...	Solicitud	Alta	Hardware Local/Equipami...	Corporativo	CERRADO	2025-09-02T12:30:38.1...	Créditos y...
Row27	163890	2025-08-20T18:19:...	Solicitud	Alta	AX Pharma 365 - GMP NO	Corporativo	CERRADO	2025-08-28T17:07:40.2...	Logística

Figura 27. Data a utilizar para el análisis de datos del MTTR en KNIME

Fuente: Elaboración Propia

- Resultados de encuesta estructurada

Los resultados de la encuesta se reciben por medio de la herramienta Microsoft Forms, la cual de manera nativa trae compatibilidad con Microsoft Excel y le permite automáticamente ingresar todas las respuestas que se ingresen al enlace original. Una vez que fue descargado el reporte, fue necesario cambiar nombres de columnas para que reflejaran lo que se inscribió originalmente en el diccionario de datos, como se muestra en las figuras 11 y 12.

Una vez que las variables habían cambiado de nombre para reflejar lo planteado en el

diccionario de datos, se hizo el mismo procedimiento que se realizó para el reporte de tickets; ingresando el archivo dentro del lector de Excel en la herramienta KNIME para luego aplicar un filtro de columnas que permitía excluir todas las variables que no se necesiten para el estudio y generación de diferentes gráficos, como es mostrado en las figuras 33 y 34.

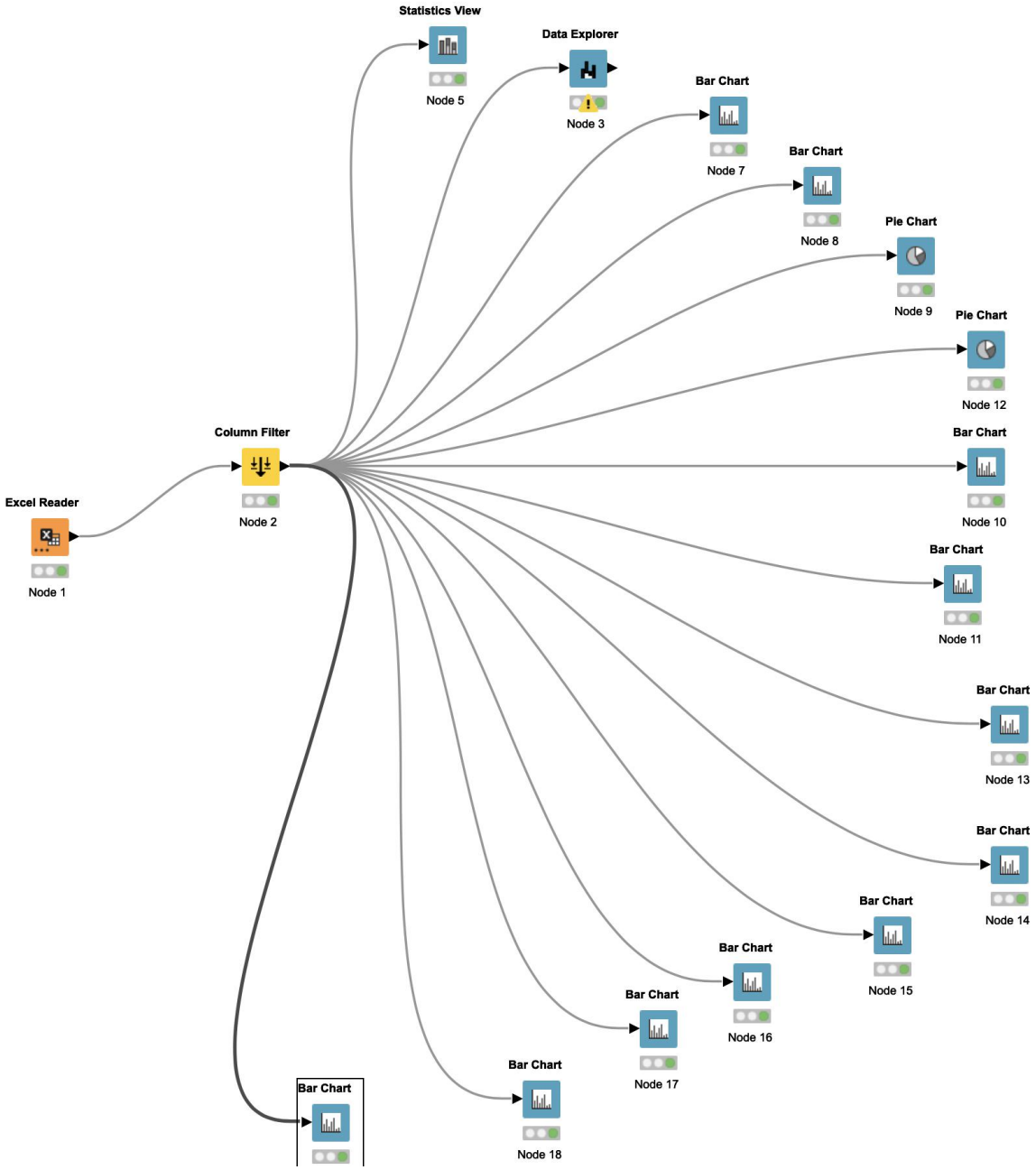


Figura 28. Esquema general para el análisis de datos del sistema de encuesta en KNIME

Fuente: Elaboración Propia

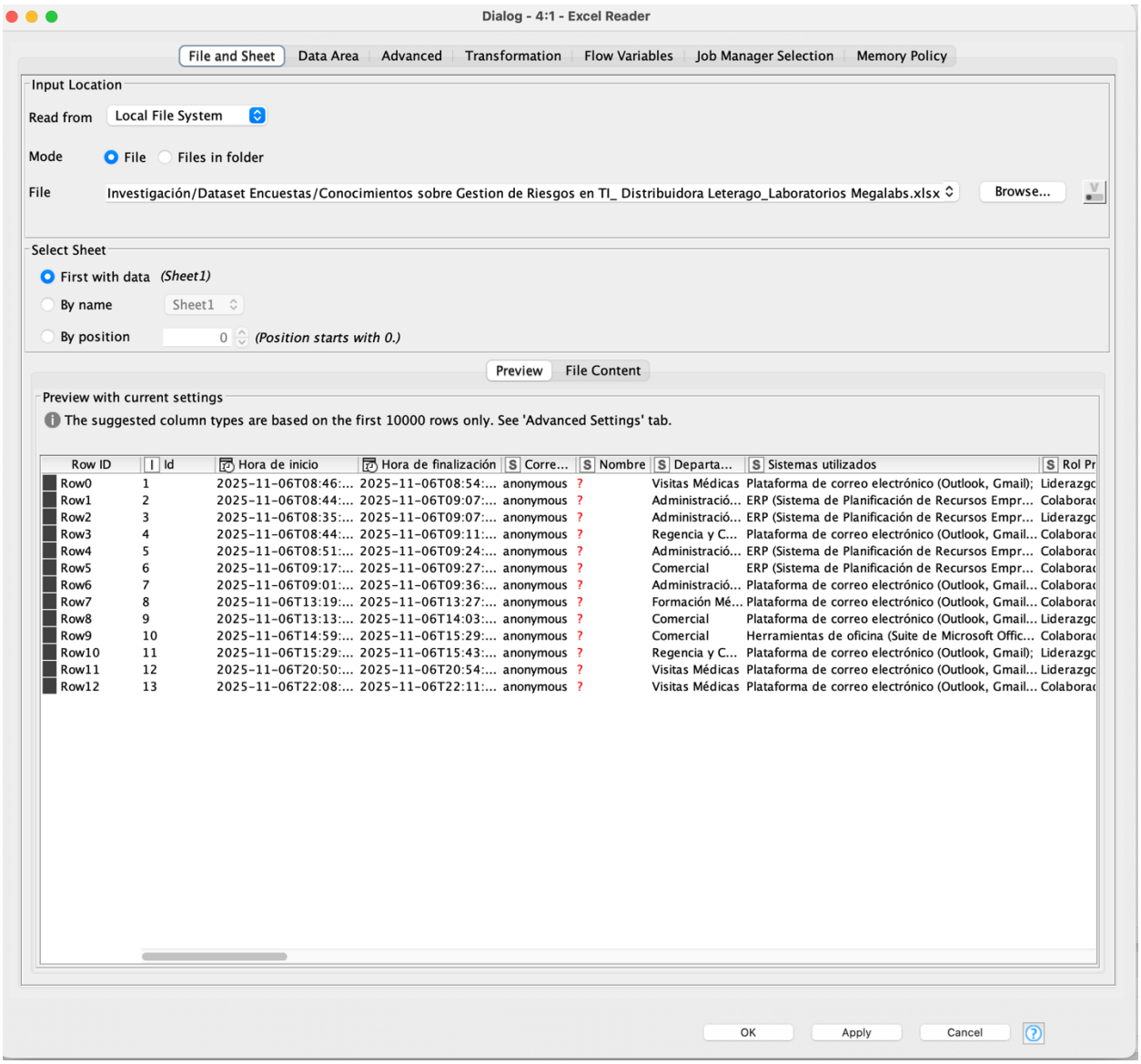


Figura 29. Data a utilizar para el análisis de datos de la encuesta estructurada en KNIME

Fuente: Elaboración Propia

4.2.1 DESCRIPCIÓN DEL PROCESO

- **Reporte de Tickets**
    - **Etapa**: Búsqueda y filtrado de reporte
        - **Tiempo**: 3 días
        - **Recursos utilizados**: Plataforma Tickets
    - **Etapa**: Extracción de reporte

        - **Tiempo**: 1 día
        - **Recurso utilizado:** Plataforma Tickets
    - **Etapa**: Limpieza de datos provenientes del reporte
        - **Tiempo:** 4 días
        - **Recurso utilizado:** Microsoft Excel, Knime
    - **Etapa**: Procesamiento y análisis
        - **Tiempo**: 1 día
        - **Recurso utilizado:** Knime
    - **Etapa**: Creación de gráficos
        - **Tiempo**: 3 días
        - **Recurso utilizado**: Knime
- **Encuesta estructurada**
    - **Etapa**: Formulación de instrumento
        - **Tiempo**: 5 días
        - **Recurso utilizado**: Microsoft Forms
    - **Etapa**: Creación de bosquejo de instrumento
        - **Tiempo**:1 día
        - **Recurso utilizado**: Microsoft Forms
    - **Etapa**: Validación de instrumento
        - **Tiempo**: 1 semana
        - **Recurso utilizado**: Microsoft Forms, Microsoft Word
    - **Etapa**: Difusión de instrumento
        - **Tiempo**: 2 días
        - **Recurso utilizado**: Microsoft Outlook, Microsoft Forms

- **Etapa**: Extracción de respuestas
    - **Tiempo**: 2 días
    - **Recurso utilizado**: Microsoft Forms, Microsoft OneDrive, Microsoft Excel
- **Etapa**: Limpieza de datos del reporte generado
    - **Tiempo**: 2 días
    - **Recurso utilizado**: Microsoft Excel, Knime
- **Etapa**: Procesamiento y análisis
    - **Tiempo**: 2 días
    - **Recurso utilizado**: Knime
- **Etapa**: Creación de gráficos
    - **Tiempo**: 3 días
    - **Recurso utilizado**: Knime

4.2.2 PARTICIPANTES O FUENTES DE INFORMACIÓN

- Reporte de Tickets

Se tomará en cuenta como participantes todas las personas que han ingresado una solicitud de apoyo o soporte dentro de la plataforma **Tickets**, las cuales también son obligatoriamente empleados de la empresa y distribuidora Leterago y Laboratorios Megalabs, las cuales varían en su rango de edad, pero que comparten ciertas características similares, como ser trabajar en el área administrativa de la empresa, lo cual ya fue delimitado en secciones anteriores donde se definía la muestra y también donde se excluía a una persona del equipo investigativo. **(Véase Sección 3.4.4)**

- Resultados de encuesta estructurada

Se toma en cuenta todas aquellas personas que laboren en la empresa y distribuidora Leterago y Laboratorios Megalabs, que pertenezcan al área administrativa, delimitada anteriormente por medio de una lista de empleados que pertenezcan a las áreas que no se consideran como la parte operativa.

Estas personas no poseen características similares o están en un mismo rango de edad ya que son de diferentes orígenes y solo se comparte que laboren en la misma empresa. **(Véase Sección 3.4.4)**

4.2.3 INSTRUMENTOS UTILIZADOS

- Encuesta estructurada

La encuesta estructurada fue construida en Microsoft Forms, con el propósito de tener una herramienta accesible, con menores tiempos de desarrollo y mayor oportunidad de difundir hacia la muestra.

Al delimitar la información que se espera recibir del instrumento en diferentes ideas principales que corresponden a la asociación de las preguntas y objetivos con lo investigado en el marco teórico, es posible definir las secciones que comprenderá la encuesta, divididas de esta manera:

- **Sección 1:** Datos Generales
- **Sección 2:** Conocimiento y Concientización
- **Sección 3:** Evaluación de Competencias
- **Sección 4:** Experiencias y Prácticas
- **Sección 5:** Comentarios y Sugerencias

Para la **Sección 1** se recolectará información como el área en la que el usuario o sujeto de estudio labora, así como los sistemas que utiliza en su día a día, retratado por las siguientes preguntas de tipo selección:

- *Departamento en el que trabaja:*
  - Administración y Finanzas
  - Comercial
  - Personas y Cultura
  - Regencia y Calidad
  - Visitas Médicas
  - Gerencia

- Otro

- *¿Qué tipo de sistemas de TI utiliza regularmente en sus labores diarias? (Seleccione todas las que apliquen)*
    - ERP (Sistema de Planificación de Recursos Empresariales, como ser Microsoft Dynamics)
    - Plataforma de correo electrónico (Outlook, Gmail)
    - Herramientas de oficina (Suite de Microsoft Office)
    - Otro

Para la **Sección 2** se recolectó información que concierne al nivel de conocimiento que el sujeto de estudio posee a nivel general sobre la gestión de riesgos por medio de la valoración o prioridad que este le dé a diferentes situaciones o afirmaciones que se plantean sobre el manejo de tecnologías y ciberseguridad, retratadas por las siguientes preguntas que utilizan la Escala de Likert anteriormente mencionada en el primer párrafo:

- *Siguiendo una escala del 1 al 5, donde 1 representa "Nada Importante" y 5 representa "Muy Importante", califique las siguientes afirmaciones según su criterio personal:*
    - ***La ciberseguridad y la gestión de riesgos de TI para contribuir a la eficiencia operativa de la empresa.***
    - ***La ciberseguridad debe ser para proteger los datos de clientes y proveedores.***
    - ***Se debe contar con un plan de recuperación ante desastres orientados al área de TI.***
    - ***Capacitar continuamente al personal en riesgos cibernéticos.***
- *Siguiendo una escala del 1 al 5, donde 1 representa "Nada Urgente" y 5 representa "Muy Urgente", califique las siguientes situaciones según su criterio personal:*
    - ***Un ataque de ransomware que bloquee el acceso a los sistemas de pedidos e inventario.***

- ***Una filtración de datos confidenciales de clientes o productos.***
- ***La caída prolongada del sistema ERP, impidiendo facturar o gestionar envíos.***
- ***El error humano interno (ej.: enviar un correo importante a la persona equivocada).***
- ***El incumplimiento de regulaciones farmacéuticas (ej.: trazabilidad de medicamentos).***

Para la **Sección 3** se evaluaron las competencias que se tienen acerca de la gestión de TI a nivel técnico, evaluado por medio de 3 preguntas de respuesta abierta cuyo propósito es que la muestra identifique componentes y procesos que se relacionan con la gestión de TI.

Las respuestas servirán para posteriormente ser calificadas dentro de una matriz de competencias que permita traducir los dominios de la norma ISO 27005 en ítems y habilidades observables para la interpretación de los datos.

- *Liste 3 activos tecnológicos clave de la empresa y describa los riesgos asociados a la confidencialidad, integridad y disponibilidad.*
- *¿Qué proceso seguiría en caso de detectar un virus dentro de los sistemas de la empresa (considere el ERP, el almacenamiento en la nube o las carpetas compartidas)? Detalle paso a paso su forma de evaluar el riesgo y las acciones que tomaría.*
- *En el caso hipotético de que un excompañero de trabajo filtre información sensible de la empresa, proponga 3 controles para tratar esta situación. (Tome en cuenta 3 tipos de tratamiento: Preventivo, Detección y Correctivo).*

El resultado de estas respuestas, posteriormente calificadas manualmente por medio de una escala de 1 a 5, donde 1 es nulo y 5 es experto en la temática, se considerarán para el llenado de la matriz descrita en la tabla 9.

El proceso manual de calificación de estos ítems depende del conocimiento mostrado por los encuestadores para poder valorar estas preguntas.

Para la **Sección 4** se recolectó información sobre lo que el usuario ha experimentado en el

área laboral orientado a la seguridad informática, así como los riesgos asociados a este y qué tipo de experiencia tiene con medidas de gestión de riesgos como planes de contingencia, retratado por las siguientes preguntas de tipo selección única:

- ***¿Ha recibido formación sobre cómo detectar amenazas de ciberseguridad como phishing o malware?***
    - Sí, de forma regular y actualizada.
    - Sí, pero hace mucho tiempo
    - No, nunca.
    - No estoy seguro/a.
- ***En el último año, ¿ha experimentado o presenciado algún incidente relacionado con la seguridad de la información? (ej.: correo phishing, ransomware, caída de sistemas críticos, pérdida de datos)***
    - Sí, en múltiples ocasiones.
    - Sí, en una ocasión.
    - No, nunca.
    - Prefiero no responder.
- ***Si respondió "Sí" a la pregunta anterior, ¿cómo manejó o reportó el incidente?***
    - Reporté inmediatamente al departamento de TI.
    - Lo reporté a mi supervisor/a
    - Intenté resolverlo por mi cuenta.
    - No supe qué hacer / No lo reporté.
    - No aplica.
- ***¿Con qué frecuencia realiza copias de seguridad (backups) de la información crítica de su trabajo hacia su directorio de nube asignado?***
    - Diariamente
    - Semanalmente

- Mensualmente
- Solo cuando me lo indican
- Nunca / No sé cómo hacerlo

Para la **Sección 5** se recolectarán las opiniones y percepciones que el usuario tiene sobre la gestión de riesgos de TI orientado a la manera en la que la empresa puede implementar o mejorar como retroalimentación, siendo esta parte cualitativa con preguntas abiertas que pretenden obtener un discernimiento mayor del sujeto de estudio, retratado por lo siguiente:

- ***Desde su perspectiva, ¿cuál es el mayor riesgo de TI al que se enfrenta nuestra empresa?***
- ***¿Qué tipo de apoyo, recursos o capacitación cree que necesita para contribuir mejor a la seguridad de la información de la empresa?***

4.2.4 DIFICULTADES ENCONTRADAS

- **REPORTE DE TICKETS**

La mayor dificultad encontrada dentro del reporte de tickets fue delimitar un período de tiempo que fuera representativo de todas las actividades que se realizan en la empresa, para lo cual se solicitó una orientación de parte del profesor que imparte la clase de Trabajo Final de Investigación y de la familiarización con el sistema previo a exportar los datos,

De igual manera, darle formato y buscar las variables que fueran de uso práctico para el equipo investigativo no era posible sin un análisis exploratorio previo de los datos dentro del sistema para poder comprender cuáles son las variables que el reporte contiene previo a hacer diferentes cálculos o modificaciones.

- **RESULTADOS DE ENCUESTA ESTRUCTURADA**

Al recolectar datos de la encuesta se encontraron varias dificultades, entre ellas, encontrar que las personas tuvieran una motivación para poder llenarlo, ya que muchas estaban preocupadas por el uso que se les podría dar a sus datos personales, para lo cual se explicó que estos datos serán utilizados de manera anónima sin tener en cuenta el nombre u otras credenciales que podrían perjudicar o poner en compromiso la situación de un empleado.

De igual manera se encontró que algunas personas de un rango mayor de edad

(aproximadamente de 40 a 50 años en adelante) eran poco receptivos al llenado de la encuesta en una plataforma digital, para lo cual se tuvo que crear un archivo imprimible que se tabuló posteriormente para incluirse dentro de los resultados.

4.2.5 CONSIDERACIONES ÉTICAS

- **REPORTE DE TICKETS**

La principal consideración ética que se debe tener para el reporte de tickets es mantener fuera todo aquello que pueda poner en compromiso; una columna que contenga identidad personal, dirección de un usuario final, nombres de personas o credenciales como el código de empleado fueron excluidos con el propósito de mantener anonimidad.

De igual manera se solicitó ante el jefe de área un permiso para poder extraer los datos del sistema, lo cual está plasmado en la Carta de Autorización de Uso de Datos adjunta en los anexos de este documento, que permite que los investigadores utilicen toda la información y todos los instrumentos o fuentes de información que se tenían identificados desde el momento de la creación del documento de trabajo final.

- **RESULTADOS DE ENCUESTA ESTRUCTURADA**

Al igual que el reporte de tickets, se debe tener una consideración ética, pero en este caso de mayor gravedad, debido a que una encuesta puede recolectar el nombre completo o datos de una persona; por lo cual, de la misma manera en la que se hizo para el reporte de tickets, se excluyen los nombres, el correo electrónico de las personas u otras credenciales que podrían poner en compromiso o daños perjudiciales hacia la muestra.

De igual manera se solicitó una carta de autorización de uso de datos para que los investigadores utilizarán esta información de manera libre en sus investigaciones y se les pregunta antes de solicitar el llenado de la encuesta si están de acuerdo con qué los datos que ellos respondan se utilicen para este estudio.

4.3 RESULTADOS Y ANÁLISIS DE LAS TÉCNICAS APLICADAS

La siguiente sección tiene como propósito plasmar la interpretación de los diferentes hallazgos por parte del equipo investigativo.

Esto comprende los dos tipos de análisis correspondientes al enfoque mixto; la presentación de los resultados cuantitativos y el análisis cualitativo son fundamentales para

posteriormente hacer la triangulación de datos, cuyo proceso permitirá poder generar conocimiento a través de la formulación de conclusiones, recomendaciones y propuestas aplicables al contexto organizacional.

4.3.1 RESULTADOS CUANTITATIVOS

Como punto inicial, se realizó un procesamiento de respuestas que corresponden a la aplicación de la matriz de competencias basada en ISO 27005, como fue detallada en la **sección 4.2.3.**

Especificando con un mayor detalle, se recolectaron todas las respuestas de la Sección 3 de la encuesta estructurada y se calificaron en base a la *evidencia a considerar,* que representa el lineamiento principal por el cual se mide la respuesta en un rango de 1 a 5, representando un nivel bajo a muy alto de conocimientos sobre la gestión de riesgos de seguridad de la información. Ver tabla 23.

Tabla 23. Matriz de evaluación de Brecha de conocimiento

Respuesta #1					
Dominio de ISO 27005	Competencia a Evaluar	Pregunta	Respuesta	Nivel de Competencia (1-5)	Evidencia a considerar
Establecimiento del Contexto	Identificar y documentar activos de información críticos del área administrativa.	Liste 3 activos tecnológicos clave de la empresa y describa los riesgos asociados a la confidencialidad, integridad y disponibilidad.	Ipad, celulares y laptop	3	Se solicitará al evaluado listar 3 activos clave y describir los riesgos asociados a su confidencialidad, integridad y disponibilidad.
Análisis de Riesgo	Aplicar técnicas para estimar la probabilidad y el impacto de amenazas identificadas (como ser correos con phishing o ransomware).	¿Qué proceso seguiría en caso de detectar un virus dentro de los sistemas de la empresa (considere el ERP, el almacenamiento en la nube o las carpetas compartidas)? Detalle paso a paso su forma de evaluar el riesgo y las acciones que tomaría.	Lo que haria es comunicarme de forma inemdiata con alguien de TI	4	El evaluado deberá explicar el proceso que seguiría para evaluar un nuevo tipo de malware que afecta al ERP.
Tratamiento del Riesgo	Conocimiento en la selección y justificación de controles de seguridad para mitigar riesgos.	En el caso hipotético de que un ex-compañero de trabajo filtre información sensible de la empresa, proponga 3 controles para tratar esta situación. (Tome en cuenta 3 tipos de tratamiento: Preventivo, Detectivo y Correctivo).	Me parece que al momento que alguien sale de la empresa debe bloqueársele todas las vias de salida de informacion que despues pueda caer en la competenecia, no es facil pero considero que se maneja bien hasta la fecha, la informacion solo la reciben en sus correos corporativos y eso da bastante seguirgad aunque no exonera que pueda haber salida de informacion clave!!!	5	Presentar un escenario de riesgo (ej. fuga de datos por un ex-empleado) y pedir que proponga 3 controles de tratamiento (preventivo, detectivo, correctivo).

Fuente. Elaboración propia.

Como es posible ver en la figura anteriormente mostrada, se utilizan 3 preguntas que corresponden a la evaluación de 3 competencias que finalmente derivan en la evaluación de 3 dominios principales de la norma ISO 27005: ***Establecimiento del Contexto, Análisis de Riesgo*** y ***Tratamiento del Riesgo.***

El procesamiento de las respuestas de todos los encuestados derivó en la formulación de 3

valores clave para poder medir cuantitativamente la brecha de conocimiento existente:

- **Promedio de Establecimiento del Contexto**
    - Resultado de evaluar la pregunta "***Liste 3 activos tecnológicos clave de la empresa y describa los riesgos asociados a la confidencialidad, integridad y disponibilidad",*** que corresponde a la competencia "***Identificar y documentar activos de información críticos del área administrativa".***
- **Promedio de Análisis de Riesgo**
    - Resultado de evaluar la pregunta ***"¿Qué proceso seguiría en caso de detectar un virus dentro de los sistemas de la empresa (considere el ERP, el almacenamiento en la nube o las carpetas compartidas)? Detalle paso a paso su forma de evaluar el riesgo y las acciones que tomaría",*** que corresponde a la competencia ***"Aplicar técnicas para estimar la probabilidad y el impacto de amenazas identificadas (como ser correos con phishing o ransomware)".***
- **Promedio de Tratamiento de Riesgo**
    - Resultado de evaluar la pregunta ***"En el caso hipotético de que un excompañero de trabajo filtre información sensible de la empresa, proponga 3 controles para tratar esta situación. (Tome en cuenta 3 tipos de tratamiento: Preventivo, Detección y Correctivo)",*** que corresponde a la competencia ***"Conocimiento en la selección y justificación de controles de seguridad para mitigar riesgos".***

Estos 3 valores clave fueron obtenidos por medio del cálculo del promedio de cada una de las calificaciones asignadas, lo cual permitió una vez obtenidas, promediarse para obtener una **Calificación Final,** que correspondería al valor medible de la Brecha de Conocimiento.

Tabla 24. Evaluación de brecha de conocimiento - promedios

Promedio de Establecimiento del Contexto	2.9
Promedio de Análisis de Riesgo	3.6
Promedio de Tratamiento de Riesgo	3.15
Calificación Final	3.21667

Fuente. Evaluación propia.

Dentro de la herramienta KNIME también se realizó una posterior exploración y análisis de esta calificación de brecha de conocimiento, valor que, si bien en la figura anterior se muestra como un total, se debe considerar que también se recibió un resultado individual por cada uno de los registros, valor que fue agregado posteriormente al set de datos transformado. Ingresar esta columna nueva dentro del contexto del set de datos es lo que permite realizar la exploración.

4.3.1.1 PRESENTACIÓN DE DATOS

Para la evaluación de los valores resultantes de la Brecha de Conocimiento, se utilizó la exploración de datos en KNIME, para lo cual arrojó una media de **3.25** de posibles 5 puntos, por lo cual se puede considerar en base a la escala definida en las secciones anteriores como un nivel de conocimiento **moderado**, se puede decir que se llega a un nivel competente, sin embargo, ocurren ciertas falencias.

Tabla 25. Datos estadísticos de la calificación de brecha de conocimiento.

Column	Minimum	Maximum	Mean	Standard Deviation	Variance	Skewness
Calificacion de Brecha de Conocimiento	1	5	3.25	1.3195560125058545	1.7412280701403506	-0.4952517727172591

Fuente. Elaboración propia

Al realizar el histograma de la Brecha de Conocimiento, se encuentra que la mayoría de encuestados orbita hacia los valores superiores entre **3.5 y 5**, por lo cual es posible inferir que la mayoría de los empleados posee un nivel mayor al nivel estándar (considerado por los investigadores de competencia como un puntaje 3) ante la gestión de riesgos orientada al área de TI.

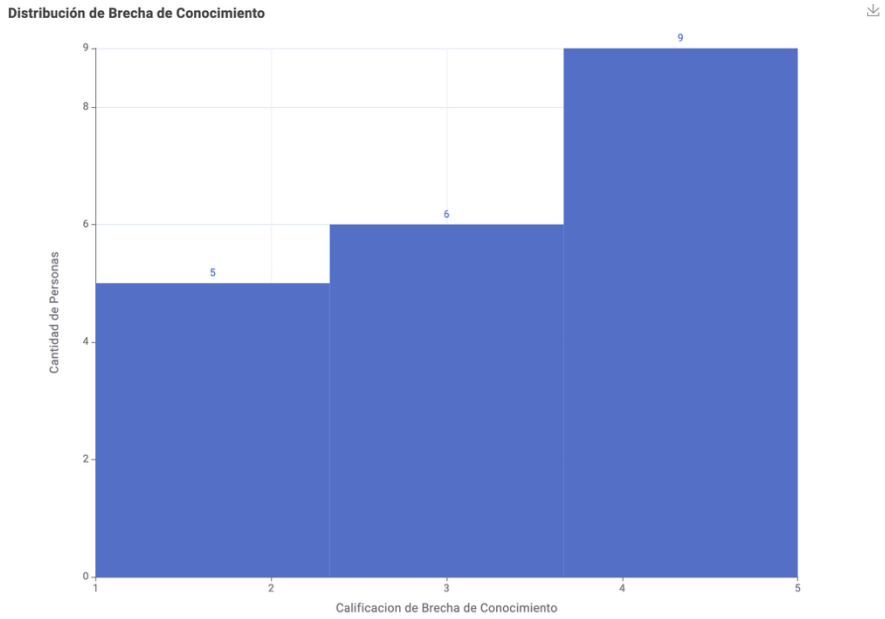


Figura 30. Distribución de la brecha de conocimiento por encuestados

Fuente. Elaboración propia.

4.3.1.2 DESCRIPCIÓN DE LOS HALLAZGOS

Como la figura del cálculo de la **Calificación Final (tabla 24)** y el promedio de todos los dominios evaluados de la ISO 27005 muestra, existen ciertas falencias dentro de las competencias evaluadas; considerando que el promedio del **Establecimiento del Contexto** es de **2.9 puntos de posibles 5**, lo cual permite inferir que los empleados de Distribuidora Leterago y Laboratorios Megalabs tienen una dificultad de considerable escala a la hora de identificar el entorno tecnológico y su gestión correcta.

Los 2 valores clave restantes, que corresponden a los promedios del **Análisis del Riesgo y Tratamiento del Riesgo**, devuelven valores de **3.6 y 3.15 puntos de posibles 5,** respectivamente, lo que permite indicar que los empleados de Distribuidora Leterago y Laboratorios Megalabs

tienen un nivel moderado de competencia por encima del promedio que les permite tener un entendimiento del cuidado de los activos del área de TI.

Asimismo, al evaluar el promedio de la calificación final de la Brecha de Conocimiento segmentado por el tipo de Rol que el empleado desarrolla en la empresa, se encontró que el Colaborador que posee ***tareas administrativas y de soporte*** es el que mejor calificación obtuvo, con un **puntaje de 3.33 de posibles 5,** seguido de los **colaboradores técnicos o especializados,** que obtuvieron **3.28 de posibles 5**, finalmente con aquellos colaboradores que están en puestos de **liderazgo o supervisión** con un **3.17 de posibles 5,** lo cual permite inferir que aquellas personas que interactúan mayor tiempo con el entorno tecnológico de la empresa van a estar informados sobre cómo gestionar y tratar los riesgos asociados a los activos del área de TI.

Comúnmente, las personas en posiciones de liderazgo o supervisión poseen otras habilidades no relacionadas al uso directo del entorno tecnológico, pues sus funciones diarias y asignaciones a largo plazo dependen no del uso directo, sino del aseguramiento y coordinación para que estas operaciones sean eficientes con un margen de provecho. Se puede decir que no es una cuestión de conocimiento, sino de aplicación de habilidades.

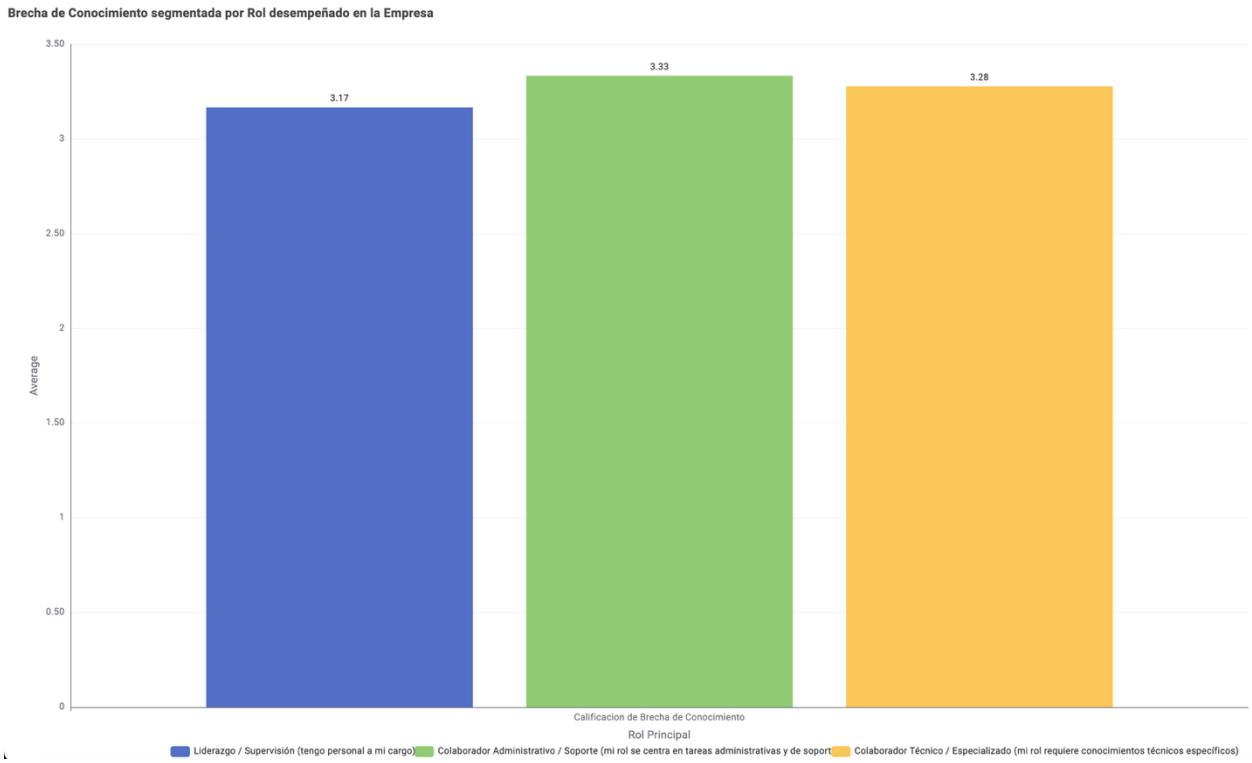


Figura 31. Brecha de Conocimiento por rol

Fuente. Elaboración propia.

4.3.1.3 RELACIÓN CON LOS OBJETIVOS

El análisis estadístico presentado a lo largo del capítulo IV busca solventar a cada uno de nuestros objetivos planteados en el capítulo I sección 1.5, acorde a la encuesta, presentada en anexos, la sección 2 es la que se enfoca en determinar datos cuantitativos, que se relacionan con los objetivos de la siguiente manera, ver tabla 26:

Tabla 26. Relación de Datos cuantitativos evaluados en la encuesta con los objetivos de la investigación

Objetivo del Proyecto	**Pregunta relacionada con el objetivo**	**Comentario de Relación**
OBJETIVO GENERAL		
Determinar el nivel de conocimiento sobre gestión de riesgos de la seguridad de la información, (M) utilizando una matriz de competencias basada en ISO 27005 y (A) encuestas a todo el personal del área, (R) para cuantificar la brecha de habilidades, (T) en un plazo de cinco semanas.	Todas las preguntas de la Sección 2	Proporcionar datos cuantitativos sobre percepciones que evidencian el nivel de concientización, lo cual es un indicador directo de la brecha de conocimiento y su posible impacto en la eficiencia operativa.
OBJETIVO ESPECÍFICO 1		
Diagnosticar la brecha de conocimiento en la gestión de riesgos de la seguridad de la información del área de TI de Distribuidora Leterago para determinar su impacto en la exposición a vulnerabilidades y la eficiencia operativa, (M) mediante encuestas y análisis documental de reportes de incidentes, (R) para generar un diagnóstico base que informe futuras estrategias de mitigación, (T) durante el último trimestre de 2025.	• La ciberseguridad y la gestión de riesgos de TI para contribuir a la eficiencia operativa de la empresa. • La ciberseguridad debe ser para proteger los	Medir el conocimiento conceptual sobre aspectos clave de la gestión de riesgos (confidencialidad, disponibilidad, continuidad) que forman parte de los dominios de ISO 27005.

Objetivo del Proyecto	Pregunta relacionada con el objetivo	Comentario de Relación
	datos de clientes y proveedores. • Se debe contar con un plan de recuperación ante desastres orientados al área de TI. • Capacitar continuamente al personal en riesgos cibernéticos.	
OBJETIVO ESPECÍFICO 2		
Identificar los factores organizacionales que perpetúan la brecha de conocimiento, (M) mediante el análisis de la documentación de políticas y (A) encuestas con los líderes de equipo, (R) para comprender las causas raíz culturales, (T) en un plazo de seis semanas.	• Capacitar continuamente al personal en riesgos cibernéticos. • El error humano interno (ej.: enviar un correo importante a la persona equivocada). • El incumplimiento de regulaciones farmacéuticas (ej.: trazabilidad de medicamentos).	Evaluar la percepción sobre la importancia de la capacitación (factor cultural) y la conciencia sobre riesgos organizacionales como el error humano y el cumplimiento normativo.

Objetivo del Proyecto	Pregunta relacionada con el objetivo	Comentario de Relación
OBJETIVO ESPECÍFICO 3		
Determinar el nivel de eficiencia operativa por medio de la respuesta a incidentes, (M) analizando el Tiempo Medio de Respuesta (MTTR) de los (A) incidentes reportados en los últimos 12 meses, (R) para conectar la brecha de conocimiento con resultados operativos, (T) en un plazo de ocho semanas.	• Un ataque de ransomware que bloquee el acceso a los sistemas de pedidos e inventario. • La caída prolongada del sistema ERP, impidiendo facturar o gestionar envíos. • Una filtración de datos confidenciales de clientes o productos.	Medir la percepción de urgencia ante incidentes que directamente afectan la eficiencia operativa, lo que se correlaciona con métricas como MTTR.

Fuente: Elaboración propia

4.3.1.4 ANÁLISIS ESTADÍSTICO

El análisis estadístico realizado recae fuertemente en la evaluación de nuestras hipótesis, reiterando que nuestra investigación se desarrolla con un enfoque mixto, se vuelve imperativo analizar su nulidad o efectividad, con el método estadístico de "Chi Cuadrado" , definida por Siegel & Castellán (1995) como "Una prueba no paramétrica que permite determinar si existe una relación estadísticamente significativa entre dos variables categóricas, comparando la tabla de frecuencias observadas con una tabla de frecuencias esperadas bajo el supuesto de independencia."

Para este propósito se utilizará el software Knime, haciendo uso de los siguientes nodos:

- **NUMERIC BINNER:** Este nodo ayuda a que cada columna se le pueda definir una serie de intervalos, conocidos como "bins". A cada uno de estos intervalos se

le asigna un nombre único (para esta columna), un rango definido y bordes de intervalo abiertos o cerrados. En pocas palabras nos ayuda a la categorización de variables de tipo numérico. (Knime, s/f-c)

- **CROSSTAB:** Este nodo de acuerdo a la página web oficial de Knime (s/f-a)
    - Crea una tabla cruzada (también conocida como tabla de contingencia o tabla de referencias cruzadas). Se puede utilizar para analizar la relación de dos columnas con datos categóricos y muestra la distribución de frecuencia de las variables categóricas en una tabla.
    - Este nodo proporciona estadísticas de prueba de **chi-cuadrado** y, en caso de una tabulación cruzada de dimensión 2x2, la prueba exacta de Fisher. Ambas estadísticas prueban la hipótesis nula de que no hay asociación entre la variable de fila y la variable de columna. Los valores p se proporcionan en la vista y en el segundo puerto de salida.
- **DECISION TREE LEARNER:** Este nodo induce un árbol de decisiones de clasificación en la memoria principal. El atributo objetivo debe ser nominal. Los otros atributos utilizados para la toma de decisiones pueden ser nominales o numéricos. Las divisiones numéricas son siempre binarias (dos resultados), dividiendo el dominio en dos particiones en un punto de división dado. Las divisiones nominales pueden ser binarias (dos resultados) o pueden tener tantos resultados como valores nominales. (Knime, s/f-b)
- **DECISION TREE PREDICTOR**: Este nodo utiliza un árbol de decisión existente (que se transmite a través del puerto del modelo) para predecir el valor de clase de nuevos patrones. (Knime, s/f-b)
- **SCORER (JAVASCRIPT):** Compara dos columnas por sus pares de valores de atributos y muestra la matriz de confusión, es decir, cuántas filas de un atributo dado coinciden con su clasificación. El diálogo permite seleccionar dos columnas para comparar; Los valores de la primera columna seleccionada se representan en

las filas de la matriz de confusión y los valores de la segunda columna en las columnas de la matriz de confusión.

La vista del nodo muestra tres tablas,

- La primera es la matriz de confusión con el número de coincidencias en cada celda. Las tasas de fila y columna pueden mostrarse mediante una configuración de configuración; son el número de predicciones correctas dividido por el número total de registros en la fila/columna. Además, es posible resaltar celdas de esta matriz para seleccionar las filas subyacentes. La selección puede pasarse a otras vistas de JavaScript.
- La segunda tabla informa de varias estadísticas específicas de una clase determinada, como Verdaderos Positivos, Falsos Positivos, Verdaderos Negativos, Falsos Negativos, Precisión, Precisión Equilibrada, Tasa de Error, Tasa de Falsos Negativos, Precisión, Sensibilidad, Especificidad, F-medida.
- La última tabla contiene estadísticas generales como la Precisión General, el Error Global, el Kappa de Cohen, los valores de Clasificado Correctamente y Clasificado Incorrectamente.

Estas tres tablas también están disponibles como puertos de salida de este nodo.(Knime, s/f-g)

- **POLYNOMIAL REGRESSION LEARNER:** Este nodo realiza regresión polinómica sobre los datos de entrada y calcula los coeficientes que minimizan el error cuadrático. El usuario debe elegir una columna como destino (variable dependiente) y varias variables independientes. Por defecto, se calculan polinomios de grado 2, que pueden cambiarse en el diálogo. (Knime, s/f-e)
- **REGRESSION PREDICTOR:** Predice la respuesta utilizando un modelo de regresión. El nodo debe estar conectado a un modelo de nodo de regresión* y a algunos datos de prueba. Solo es ejecutable si los datos de prueba contienen las columnas que utiliza el modelo aprendiz. Este nodo añade una nueva columna a la

tabla de entrada que contiene la predicción de cada fila.(Knime, s/f-f)

- **NUMERIC SCORER:** Este nodo calcula ciertas estadísticas entre los valores de una columna numérica (r Yo) y predicho (p Yo) valores. Los valores calculados pueden inspeccionarse en la vista del nodo y/o procesarse posteriormente utilizando la tabla de salida.(Knime, s/f-d)

A continuación, el flujo diagramado en knime, más la configuración por nodo para lograr este cometido, ver figura 33:

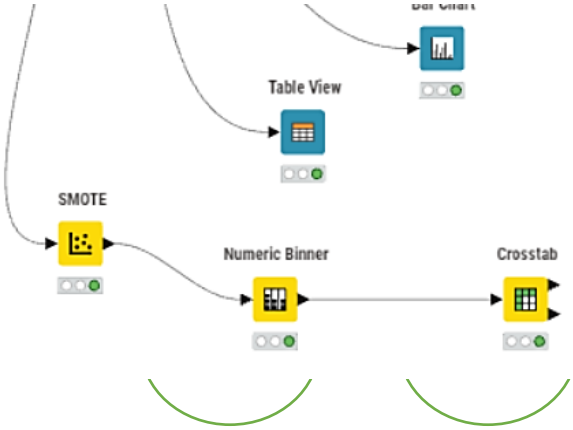


Figura 33. Flujo en Knime para cálculo de Chi Cuadrado

Fuente: Elaboración propia, software knime

Interpretación:

- Se toma la columna Departamento del dataset de encuesta como variable objetivo.

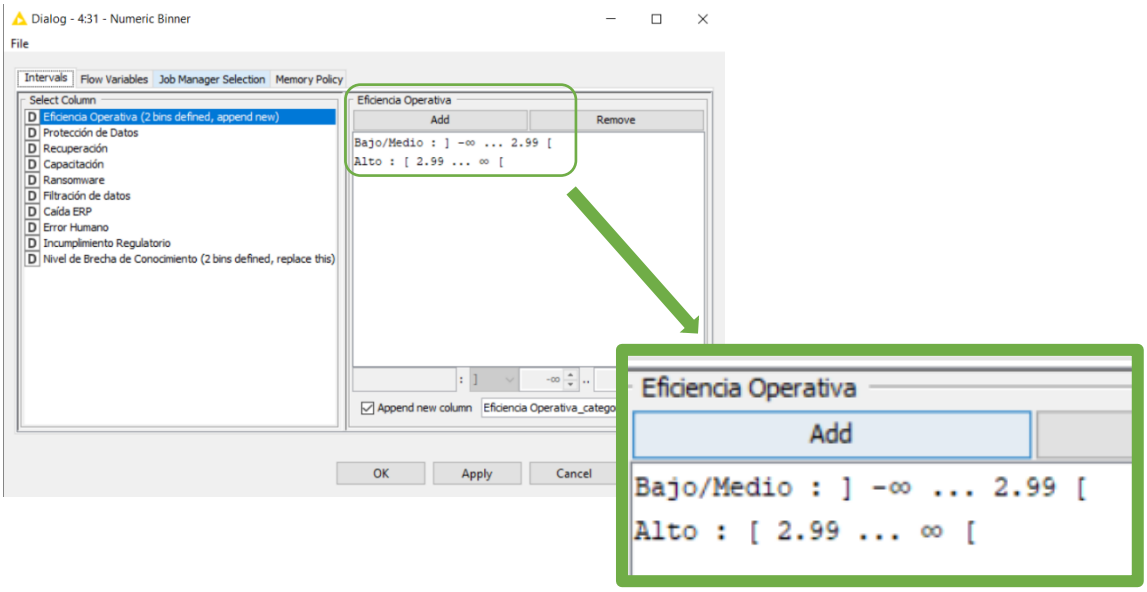


Figura 35. Configuración de NUMERIC BINNER – Categoría Eficiencia Operativa

Fuente: Elaboración propia, software Knime.

Interpretación:

- Se definen dos categorizaciones para el dato de Nivel de importancia en la Eficiencia Operativa (cálculo mostrado en sección 4.3.1)
    - Bajo/Medio: que indica que su promedio de brecha de conocimiento está en el rango de 1 a 2.99
    - Alto: que indica que su promedio de brecha de conocimiento está en el rango de 3 a 5

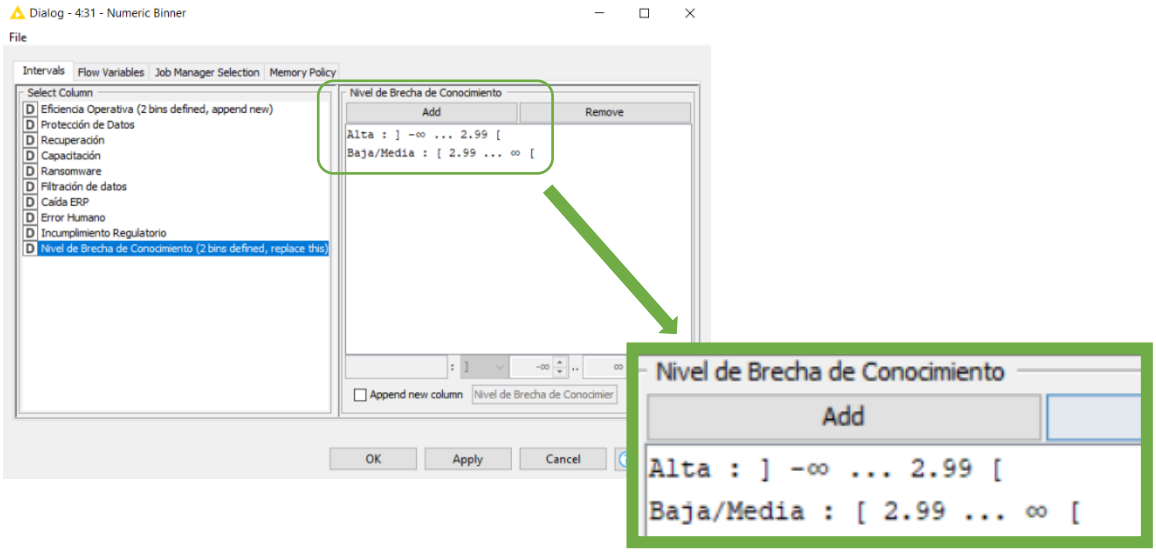


Figura 36. Configuración de NUMERIC BINNER – Categoría Brecha de Conocimiento

Fuente: Elaboración propia, software Knime.

Interpretación:

- Se definen dos categorizaciones para el dato de Brecha de conocimiento (cálculo mostrado en sección 4.3.1)
    - Alta: que indica que su promedio de brecha de conocimiento está en el rango de 1 a 2.99
    - Baja/Media: que indica que su promedio de brecha de conocimiento está en el rango de 3 a 5

Tabla 27. Ejecución de nodo CROSSTAB

Cross Tabulation of Eficiencia Operativa by Calificacion de Brecha de Conocimiento

Frequency Row Percent	Alta	Baja/Media	Total
Alto	934.5332	1,232.8401	2,167.3733
	43.1182%	56.8818%	
Bajo/Medio		70	70
		100%	
Total	934.5332	1,302.8401	2,237.3733

☑ Frequency
☐ Expected
☐ Deviation
☐ Percent
☑ Row Percent
☐ Column Percent
☐ Cell Chi-Square

Max rows: 10

Max columns: 10

Statistics for Table of Eficiencia Operativa by Calificacion de Brecha de Conocimiento

Statistic	DF	Value	Prob
Chi-Square	1	22.5946	2.00E-6

Total sample size: 2237.373336649547

Fuente. Elaboración propia, software Knime

Interpretación:

La tabla cruza:

- Eficiencia Operativa: Alto y Bajo/Medio
- Nivel de Brecha de Conocimiento: Alta y Baja/Media

Conclusiones preliminares:

- La mayoría (56.9%) de quienes consideran importante la Eficiencia Operativa (Alto) presentan un Nivel de Brecha de Conocimiento (Baja/Media), lo cual tiene sentido, a menor brecha de conocimiento en gestión de riesgos de TI correspondería

una consideración importante en su relación con Eficiencia Operativa.

- Sin embargo, aquellos casos donde la Eficiencia Operativa se considera poco importante (Bajo/Media) también presentan un Nivel de Brecha Baja/Media de Conocimiento (100%)

Tabla 28. Ejecución de nodo NUMERIC SCORER

R²:	0.996
Mean absolute error:	29.238
Mean squared error:	854.887
Root mean squared error:	29.238
Mean signed difference:	-9.746
Mean absolute percentage error:	0.158
Adjusted R²:	0.996

Fuente. Elaboración propia, software Knime

Interpretación:

- Al utilizar el nodo Numeric Scorer, es posible extraer la siguiente información que corresponde a la evaluación de la efectividad que tiene el modelo de chi-cuadrado en ser predictivo, por lo cual, el valor R^2, siendo de un valor de **0.996** corresponde a la medición del poder explicativo del modelo, considerado a un nivel alto porque es capaz de explicar el **99.6%** de la varianza de la variable dependiente, que corresponde a la Eficiencia Operativa.
- El error porcentual absoluto medio (MAPE, por sus siglas inglés) es de **15.8%,** por lo que representa una precisión considerable en base a la escala de medición, en cuanto al error absoluto medio (MAE, por sus silgas en inglés) siendo de 29.24 indica que la distribución de errores es simétrica, con pocos o ningún valor atípico que distorsione la predicción.

Conclusiones preliminares:

- Es posible decir que el modelo creado para su evaluación de chi-cuadrado demuestra que tiene una capacidad alta para identificar si las dos variables tienen una relación que les defina.

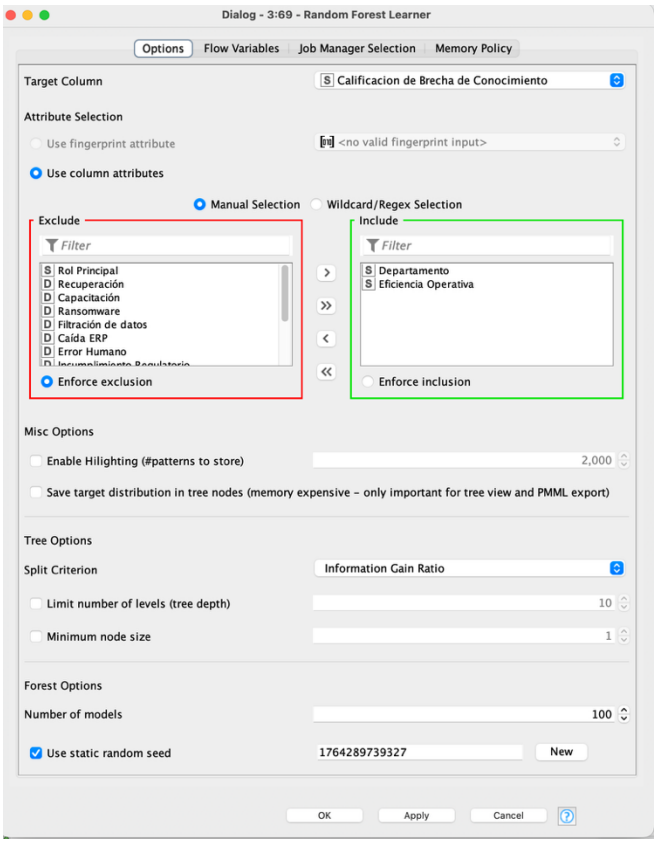


Figura 38. Flujo de algoritmo predictivo – Random Forest

Fuente. Elaboración propia, software Knime

Interpretación

- El nodo se configuró para evaluar la variable Calificación de Brecha de Conocimiento, con el objetivo de analizar la relación que existe sobre la percepción de la eficiencia operativa de la empresa, junto con el departamento en donde labora la muestra tomada.

Tabla 29. Matriz de confusión

Matriz de Confusión

Confusion Matrix

	Alta (Predicted)	Baja/Media (Predicted)	
Alta (Actual)	161	20	88.95%
Baja/Media (Actual)	40	247	86.06%
	80.10%	92.51%	

Overall Statistics

Overall Accuracy	Overall Error	Cohen's kappa (κ)	Correctly Classified	Incorrectly Classified
87.18%	12.82%	0.735	408	60

Fuente. Elaboración propia, software Knime

Interpretación:

- El modelo presenta un excelente rendimiento bajo el análisis de las variables utilizadas, Brecha de conocimiento y Eficiencia operativa, teniendo una capacidad discriminativa muy fuerte entre sí.
- Existe un alto nivel de precisión global, con un 87.18%, explicado por su alta tasa de excelente reconocimiento entre la Brecha de Conocimiento para las dos clases, aunque tiene un mejor porcentaje para la clase *Baja/Media.*
- El coeficiente de Kappa es de 0.735, lo que significa que las respuestas esperadas tienen una concordancia más allá del azar.

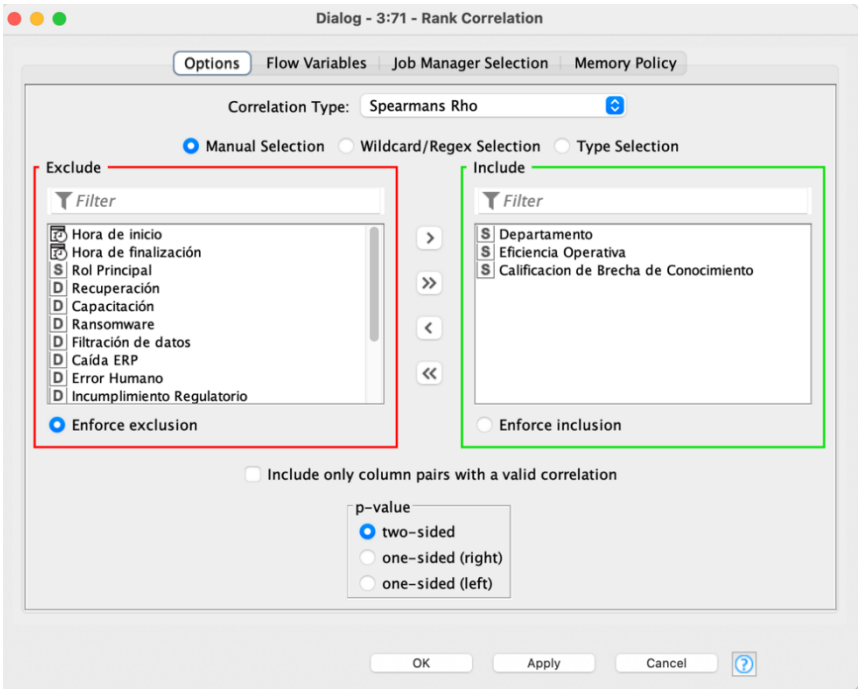


Figura 39. Configuración del nodo Rank Correlation para la Prueba de Spearman

Fuente. Elaboración propia, software Knime

Tabla 30. Matriz de correlación de las variables Departamento, Eficiencia Operativa, Calificación de Brecha de Conocimiento

First column name *String*	Second column name *String*	Correlation value *Number (Float)*	p value *Number (Float)*	Degrees of freedom *Number (Integer)*
Departamento	Eficiencia Operativa	-0.025	0.588	466
Departamento	Calificacion de Brecha de Conocimiento	-0.462	0	466
Eficiencia Operativa	Calificacion de Brecha de Conocimiento	0.145	0.002	466

Fuente. Elaboración propia, software Knime

Interpretación:

La prueba de Spearman determina que la relación entre el Departamento y Eficiencia Operativa no es significativa pues esta posee un valor correlacional de -0.025 y un valor $p > 0.05$

La relación entre el Departamento y la Brecha de Conocimiento es moderada teniendo esta un valor correlacional de -0.462 y un valor p igual 0.001 ($p < 0.05$). Lo que indica que las brechas de conocimiento varían significativamente entre las distintas áreas de la organización.

La relación entre Eficiencia Operativa y Brecha de Conocimiento tiene un valor correlacional de 0.145, concluyendo una relación débil pero significativa con un valor p = 0.01 ($p < 0.05$). Sugiriendo que el nivel de competencias y conocimientos relacionados con la gestión de riesgos influye, aunque ligeramente, en la eficiencia operativa del personal.

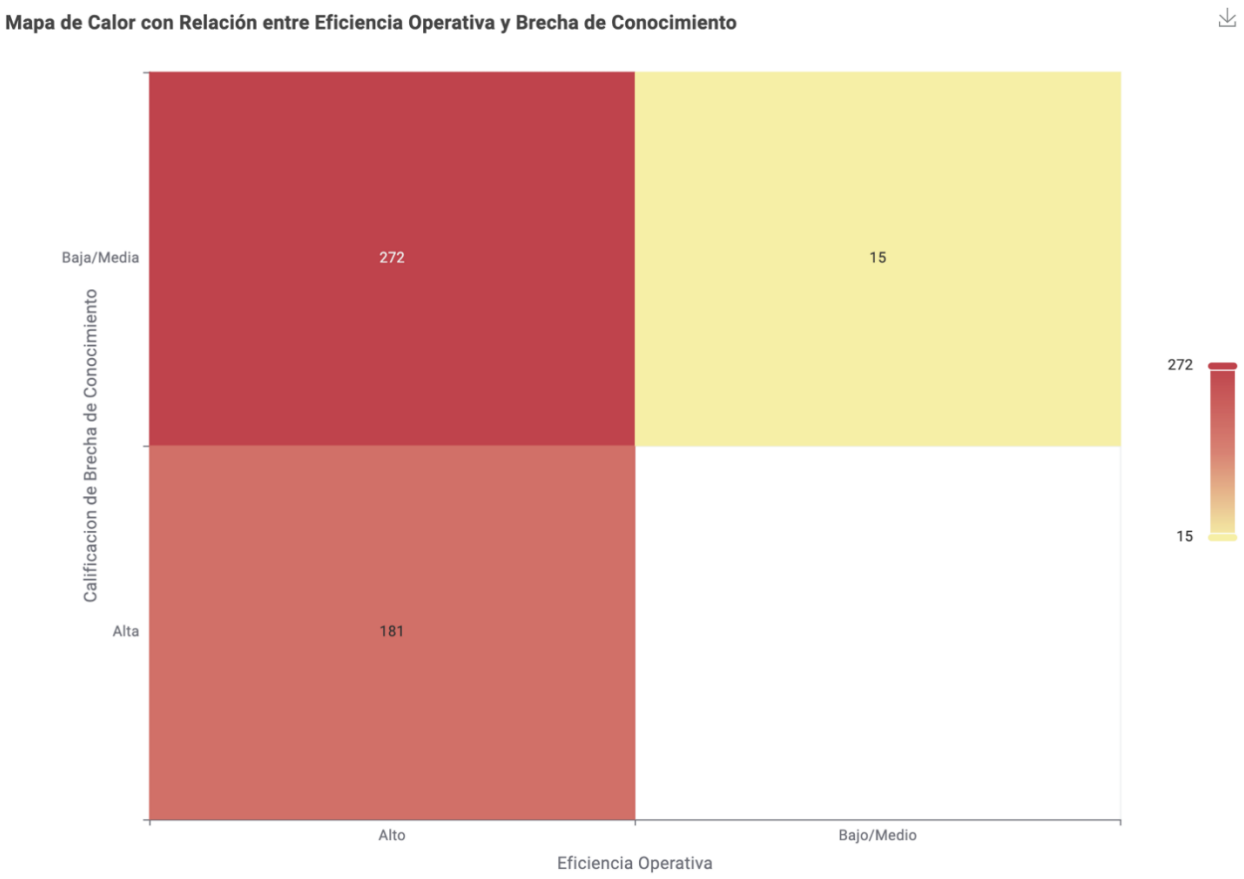


Figura 41. Mapa de calor de la relación entre eficiencia operativa y nivel de brecha de conocimiento.

Fuente. Elaboración propia, software Knime

Interpretación:

Se infiere que, a mayor Brecha de Conocimiento, menor será la consideración en la Eficiencia Operativa, y viceversa; a menor Brecha de Conocimiento, mayor será la consideración en la Eficiencia Operativa.

Para la Hipótesis 1, que relaciona la formación en ciberseguridad con el

departamento, se empleó la Prueba de Chi-Cuadrado de Independencia. La Tabla 34, nodo Cross table, muestra la distribución de frecuencias observadas, mientras que la Tabla 35 reporta el estadístico de prueba y el valor p.

El valor p significativo ($p < 0.05$) llevó a rechazar la hipótesis nula de independencia, concluyendo que existe una asociación estadísticamente significativa entre el departamento del empleado y la frecuencia de capacitación recibida.

Tabla 34. Prueba de Chi Cuadrado Formación en Ciberseguridad por Departamento

Cross Tabulation of Formación en Ciberseguridad by Departamento

Frequency Row Percent	Administración y Finanzas	Comercial	Formación Médica	Gerencia	Herramientas Digitales	Logística	Operaciones	Regencia y Calidad	TI	Visitas Médicas	Total
No estoy seguro/a.		3								4	7
		42.8571%								57.1429%	
No, nunca.	3	5	5					3		3	19
	15.7895%	26.3158%	26.3158%					15.7895%		15.7895%	
Sí, de forma regular y actualizada.					5			5	2	5	17
					29.4118%			29.4118%	11.7647%	29.4118%	
Sí, pero hace mucho tiempo	31	5		6		1	4			4	51
	60.7843%	9.8039%		11.7647%		1.9608%	7.8431%			7.8431%	
Total	34	13	5	6	5	1	4	8	2	16	94

Frequency
Expected
Deviation
Percent
Row Percent
Column Percent
Cell Chi-Square
Max rows: 10
Max columns: 10

Statistics for Table of Formación en Ciberseguridad by Departamento

Statistic	DF	Value	Prob
Chi-Square	27	84.294	8.31E-8

Total sample size: 94.0

Fuente. Elaboración propia, software knime

Tabla 35. Evaluación de prueba de chi-cuadrado

R^2:	0.606
Mean absolute error:	3.083
Mean squared error:	16.579
Root mean squared error:	4.072
Mean signed difference:	-1.807
Mean absolute percentage error:	0.624
Adjusted R^2:	0.606

Fuente. Elaboración propia, software knime

4.3.2 ANÁLISIS CUALITATIVO

Para el análisis cualitativo de los datos recolectado, se tomará mayoritariamente las respuestas de campo abierto de la encuesta estructurada, pues el propósito de ellas al formular el

instrumento fue tener una manera confiable y menos complicada de poder relacionar el enfoque mixto de la investigación.

Las respuestas que se tomarán en cuenta pertenecen a las Secciones 3 y 5 del instrumento; preguntas orientadas a obtener una visión sobre la perspectiva del colaborador ante el manejo y gestión de riesgos en el área de TI de la empresa, al mismo tiempo buscando medir la conciencia situacional de este y poder generar conclusiones o recomendaciones.

Posteriormente a la interpretación de los datos cualitativos, es posible proceder a la triangulación de datos, donde se hará la interpretación **completa** respondiendo al enfoque mixto, relacionando datos numéricos puntuales con las experiencias y percepciones de los colaboradores de la empresa teniendo en cuenta siempre el contexto planteado en el marco teórico.

4.3.2.1 CATEGORÍAS O TEMAS EMERGENTES

Para encontrar los temas y categorías más importantes, es necesario evaluar y analizar las secciones 3 y 5 de la encuesta estructurada.

Se realizó una lectura a fondo, tomando notas y extrayendo temas que fueran frecuentemente mencionados por la muestra, que si bien comprenden una pequeña parte de lo atendido por el instrumento, dejan entrever la percepción que se tiene no solo a nivel de gestión de riesgos en el área de TI, sino a gran escala sobre el papel que desempeña el área de TI dentro de la empresa como tal y como este crea una experiencia tecnológica para las diferentes áreas, en donde en última instancia, el sentimiento y la necesidad de un entorno tecnológico seguro y moderno impera sobre la organización.

Es posible delimitar los temas principales a los siguientes:

- ***La comunicación del usuario final hacia el área de TI***
- ***La percepción de vulnerabilidad***
- ***La implementación y cumplimiento de políticas de seguridad***
- ***La necesidad de capacitaciones orientadas al uso correcto de la tecnología en el entorno laboral***

4.3.2.2 CITAS O EJEMPLOS

La siguiente sección tiene como propósito retratar y evidenciar pruebas de los temas

principales retratados en la sección anterior, para justificar la categorización correspondiente.

- ***La comunicación del usuario final hacia el área de TI***
    - Diferentes colaboradores que respondieron la encuesta mencionaron muchas veces como respuesta a la pregunta de la Sección 3 *"¿Qué proceso seguiría en caso de detectar un virus dentro de los sistemas de la empresa (considere el ERP, el almacenamiento en la nube o las carpetas compartidas)? Detalle paso a paso su forma de evaluar el riesgo y las acciones que tomaría",* comunicarse con el área de TI para obtener respuestas o asistencia en caso de sufrir pérdidas u otras situaciones derivadas de la detección de un virus, como fue retratado por la Respuesta #10, donde comunica que lo que haría "es comunicarse de forma inmediata con alguien de TI", o la Respuesta #10 que indica "notificar al área de seguridad informática o al responsable de TI", como ejemplos principales.
- ***La percepción de vulnerabilidad***
    - Al responder cuál es el mayor riesgo de TI que puede enfrentar la empresa, muchos de los colaboradores respondió con temas relacionados a las vulnerabilidades que ellos perciben que pueden afectar en última instancia, como ser "virus que dañe la continuidad de la operación" o "malware, phishing, ransomware, entre otros", asimismo se mencionan riesgos como la "exposición de la información", ya sea confidencial o general de la empresa, considerando uno de ellos que por la naturaleza del trabajo en campo está propenso a sufrir una filtración de información.
- ***La implementación y cumplimiento de políticas de seguridad***
    - Para la percepción de los colaboradores, ven el hecho de bloquear los accesos de una persona de manera inmediata como una prioridad, pues de ello pueden desembocar riesgos como la filtración de información.
    - De igual manera, otro colaborador propone incluso como medida de gestión de riesgo alertas automáticas cuando ocurra una acción que involucre el acceso a información.

- ***La necesidad de capacitaciones***
    - Los colaboradores ven la necesidad de capacitaciones como algo importante, considerando que las respuestas son detalladas en cuanto a lo que solicitan como temas para poder expandir sus conocimientos sobre el uso de la tecnología; respuestas como *"Mantenernos informados y actualizados cuales son las nuevas formas que podrían afectar la seguridad de la información en la empresa. Cuál es el alcance de la responsabilidad como usuario"* o *"Capacitación del uso apropiado de los recursos de la empresa y conocimiento de los riesgos existentes en este rubro"* dejan entrever que si se reconoce a todos los niveles la necesidad de que la empresa provea el conocimiento necesario para que los empleados puedan utilizar de manera eficiente la tecnología.

Tabla 30. Identificación de habilidades de los encuestados en base a sus respuestas

Tema	Pregunta Correspondiente(s)	Respuestas como evidencia
La comunicación del usuario final hacia el área de TI	¿Qué proceso seguiría en caso de detectar un virus dentro de los sistemas de la empresa (considere el ERP, el almacenamiento en la nube o las carpetas compartidas)? Detalle paso a paso su forma de evaluar el riesgo y las acciones que tomaría.	Además de reconocer a TI como la entidad pertinente para enfrentar este tipo de casos y citamos *"En caso de detectar algún virus o amenaza de este, informar inmediatamente al departamento de TI local."* Algunos usuarios van más allá conociendo medidas preventivas y correctivas a nivel de software, y citamos *"A demás está el firewall que maneja la empresa en la que ayuda a detectar aquellos correos que entran o salen, por ejemplo, que podrían representar una amenaza inminente para la empresa."*
La percepción de vulnerabilidad	Desde su perspectiva, ¿cuál es el mayor riesgo de TI al que se enfrenta la empresa?	En su mayoría las respuestas de los encuestados van acorde a vulnerabilidades en los principios del aseguramiento de la información, y citamos *"Malware, phishing, ransomware, entre otros"* *"Un ataque cibernético, que el servicio de fibra óptica en caso de*

Tema	Pregunta Correspondiente(s)	Respuestas como evidencia
		daño no sea reparado de forma inmediata" *"Al uso de la información por parte del ser humano y con malas intenciones."*
La implementación y cumplimiento de políticas de seguridad	¿Qué proceso seguiría en caso de detectar un virus dentro de los sistemas de la empresa (considere el ERP, el almacenamiento en la nube o las carpetas compartidas)? Detalle paso a paso su forma de evaluar el riesgo y las acciones que tomaría. En el caso hipotético de que un excompañero de trabajo filtre información sensible de la empresa, proponga 3 controles para tratar esta situación. (Tome en cuenta 3 tipos de tratamiento: Preventivo, Detección y Correctivo). Desde su perspectiva, ¿cuál es el mayor riesgo de TI al que se enfrenta la empresa?	En respuesta a la segunda pregunta presentada en esta sección, los encuestados reconocen la importancia de dar de baja a un usuario de todos los sistemas, inmediatamente al momento de la desvinculación laboral, y citamos "*Cambiar todas las contraseñas a las que él o ella tenía acceso, dar de baja a su usuario y eliminar sus credenciales"* *"Preventivo: eliminación o bloqueo inmediato de todos los accesos con que el excolaborador contaba* *Detección: comunicación inmediata a los responsables del resguardo de información y ejecución de bloqueos pertinentes* *Correctivo: identificación de aprendizaje e implementación de estrategias de prevención"*
La necesidad de capacitaciones	¿Qué tipo de apoyo, recursos o capacitación cree que necesita para contribuir mejor a la seguridad de la información de la empresa?	Surgen respuestas muy variadas pero muy enriquecedoras para la detección de carencias a nivel de capacitación, que pueden ayudar a la prevención de futuros problemas, y citamos. *"Mantenernos informados y actualizados cuales son las nuevas formas que podrían afectar la seguridad de la información en la empresa. Cuál es el alcance de la responsabilidad como usuario."* *"Capacitación continua en ciberseguridad y políticas sobre el manejo de la información."*

Fuente: Elaboración propia, con data de respuestas de encuestados

4.3.2.3 INTERPRETACIÓN

- ***La comunicación del usuario final hacia el área de TI***

Es destacable notar que la mayoría de los colaboradores responda con el hecho de una

acción de contacto al área de TI con el motivo de notificar una incidencia, pero, se encuentra que en la mayoría de las respuestas, los colaboradores solamente se limitan a mencionar el contacto a TI en el momento de la detección de un virus, pero no se ve un aspecto proactivo como el realizar pasos previos de protección.

"Llamar a TI" como respuesta tampoco permite evaluar del todo si el colaborador también sería capaz de compartir la información suficiente como para que el encargado del área pueda tomar decisiones en base a las incidencias que el reportan, por lo que se encuentra una cultura organizacional de dependencia técnica hacia el área de TI como único responsable de velar por la ciberseguridad, añadiendo una carga y posibles cuellos de botella en los procesos del área.

- ***La percepción de vulnerabilidad***

Las respuestas sobre la identificación de riesgos y la perspectiva sobre el cuidado de los activos permiten saber que los colaboradores de la Distribuidora Leterago y Laboratorios Megalabs tienen una noción sobre las amenazas activas que pueden afectar las operaciones donde se utilizan las herramientas que provee TI, no obstante, esta visión no se percibe como amplia al analizar las respuestas que se dan en la encuesta, donde no se mencionan amenazas digitales sofisticadas, sino un mal manejo del usuario final.

El tema de la percepción de la vulnerabilidad entra en juego con la necesidad de capacitaciones, ya que al crear programas de concientización sobre amenazas en el entorno tecnológico la percepción de vulnerabilidad se amplía en la mente del colaborador, permitiéndole entender a un mayor nivel que las amenazas no se limitan a la mala manipulación por parte de un usuario, sino cosas que pueden actuar utilizando el engaño o el desconocimiento de una tecnología.

- ***La implementación y cumplimiento de políticas de seguridad***

Al evaluar las preguntas que comprenden ese tema, solo un 30% de ellos, que representa alrededor de 6-8 personas pudieron mencionar controles detallados o políticas específicas, como ser, "*Preventivo: Segregación de funciones; los accesos deben ser de acuerdo con las funciones del usuario al igual que los accesos a la información.*

Defectivo: Alertas automáticas; Por ejemplo notificación de descarga excesiva de información o de bade de datos de clientes

Correctivo: Capacitación. sí un usuario es reiterativo con errores o su operación es

incorrecta", y, de igual manera, se reconoce que dentro de las respuestas existe un enfoque más reactivo que preventivo, donde las respuestas se centraban más en solucionar el problema existente sin tomar en cuenta los casos futuros o como sentar un precedente para dar medidas de protección.

Al no tener una estructura metodológica sólida, no hay manera que un colaborador pueda manejar el tema del impacto que una política de seguridad puede tener sobre un entorno laboral con mucha fluidez, fallando en comprender por qué la implementación de políticas preventivas es, a largo plazo, la mejor opción sobre políticas reactivas.

- ***La necesidad de capacitaciones***

Al evaluar las preguntas que pertenecen a este tema, se pueden encontrar brechas de conocimiento evidentes; respuestas como "sin respuesta" o respuestas incompletas, que comprenden alrededor de 4-5 indican que hay una falta de formación básica sobre el uso de la tecnología.

En muchas respuestas, se puede interpretar que los evaluados saben QUÉ hacer (contactar e indicar el problema o situación al área de TI) pero no CÓMO hacerlo efectivamente, por lo que se intuye que existe una escasa capacidad para analizar escenarios y proponer soluciones estructuradas.

4.3.2.4 TRIANGULACIÓN

- ***La comunicación del usuario final hacia el área de TI***

Se encuentra que, en el reporte de Tickets, la mayoría de las solicitudes de ayuda a soporte técnico son orientadas hacia el software **AX Pharma 365** (*véase la figura 11*) que utiliza la empresa para inventario y facturación, y dentro de la encuesta se evalúa que pasos realizaría en caso de ver una anomalía o incidencia en este servicio.

Al evaluar las respuestas que los colaboradores dan, es posible ver que existe una falencia a nivel de identificación del problema en específico, limitándose solamente a hacer el contacto con el área de TI; esto puede desembocar en una falta de comunicación entre el usuario final y el área de TI. Al no poder identificar correctamente el problema, puede provocar un tiempo mayor de detección y respuesta por parte del área y ralentizando la eficiencia del servicio de soporte técnico.

Se ve necesaria la implementación de capacitaciones o la concientización al usuario final sobre el funcionamiento de sus herramientas para poder mejorar el proceso de comunicación hacia

el área de TI que al final desembocaría en la mejora del tiempo promedio de respuesta.

- ***La percepción de vulnerabilidad***

Al evaluar las respuestas de los colaboradores visibles en las figuras 19, 20 y 21 de la parte cuantitativa, es posible inferir que la organización comprende la importancia y la urgencia de la implementación de controles de seguridad para evitar incidentes que podrían perjudicar la operación diaria de la empresa, donde se valora la importancia de proteger los datos de la empresa hasta la importancia de tener una plan de recuperación en una puntuación de 5 puntos, el máximo posible, por lo cual, al comparar los datos con la fundamentación de esta respuestas en la sección cualitativa, se encuentra que, si bien todos comprenden la importancia, su nivel de conocimiento varía.

Desde respuestas donde se mencionan los tipos de amenaza más frecuente (como ser malware o phishing) hasta riesgos externos, las respuestas de los colaboradores dejan entrever que se conoce más sobre el mal manejo del usuario final de las tecnologías más que de amenazas sofisticadas como ataques tecnológicos.

Esta percepción de vulnerabilidad puede ser ampliada en su alcance por medio de programas de concientización o capacitaciones orientadas al usuario final.

- ***La implementación y cumplimiento de políticas de seguridad***

Las figuras 19, 20 y 21 no solamente dan una percepción de la vulnerabilidad, sino que también se relacionan con las políticas de seguridad; la protección de datos y los planes de recuperación son el resultado del desarrollo de políticas de seguridad; viéndolo en la parte cualitativa, se vuelve a mencionar que las respuestas de los colaboradores dejan entrever que, si bien conocen sobre el resultado de las políticas de seguridad, su entendimiento se limita hasta cierto nivel de detalle y especificación.

La falta de respuestas donde expliquen más a detalle un procedimiento y el enfoque de acciones reactivas sobre preventivas permiten inferir que existe una brecha significativa entre la valoración teórica de las políticas sobre la capacidad práctica para implementarlas.

La tabla 24 muestra las calificaciones recibidas sobre la valoración de la matriz de competencias, en donde el ítem **Establecimiento del Contexto** posee una calificación de 2.9 puntos sobre 5 posibles, y, las respuestas en el ámbito cualitativo reflejan siempre acciones de

contención y procederes reactivos.

Al existir una falencia en la comprensión del entorno tecnológico y el uso eficiente de los activos del área de TI, se comprende por qué existe una debilidad en establecer el contexto y explica por qué las políticas definidas de seguridad no se implementan efectivamente o no se hacen parte de la cultura organizacional con tanta facilidad.

- ***La necesidad de capacitaciones***

El deseo imperante de ampliar los conocimientos por medio de las capacitaciones no solo es un tema que se ve de manera cualitativa.

En el caso de la figura 21, que muestra el nivel de importancia que consideran los encuestados sobre recibir capacitaciones constantes en temas de ciberseguridad con el propósito de mantener un conocimiento sobre la gestión de TI y sus activos, 3 áreas (**Administración y Finanzas, Regencia y Calidad, Área Comercial)** consideraron que era muy importante **(puntuación de 5).**

En el caso de la parte cualitativa, surgen respuestas muy variadas pero muy enriquecedoras para la detección de carencias a nivel de capacitación, que pueden ayudar a la prevención de futuros problemas, y se cita:

"Mantenernos informados y actualizados cuales son las nuevas formas que podrían afectar la seguridad de la información en la empresa. Cuál es el alcance de la responsabilidad como usuario."

Por medio de ideas como *"Capacitación del uso apropiado de los recursos de la empresa y conocimiento de los riesgos existentes en este rubro" o "Capacitación continua en ciberseguridad y políticas sobre el manejo de la información."*, se permite plantear la idea de que la necesidades de capacitaciones trasciende algo que se pueda considerar como subjetivo y se consolida como una necesidad a futuro para mantener el control de factores de cultura organizacional y el uso que se le da a la tecnología en el entorno laboral.

4.4 ANÁLISIS INFERENCIAL Y MODELOS APLICADOS

En la siguiente sección de este documento se procederá a utilizar principalmente pruebas estadísticas y la creación de modelos para poder empezar a formular ideas y proposiciones que permitan la formación posterior de conclusiones y recomendaciones basadas en datos puntuales e

interpretación y triangulación de las fuentes de datos recolectadas hasta el momento.

4.4.1 ANÁLISIS INFERENCIAL

Existe una relación significativa en ambas hipótesis, confirmadas estadísticamente; así como la brecha de conocimiento y el departamento influye en la percepción de la eficiencia operativa, se puede afirmar que también existen diferencias reales entre la frecuencia de capacitación entre departamentos que, en última instancia, afecta en la gestión de riesgos como un todo. Esta relación fue probada con un nivel de confianza del 95%, para asegurar una alta fiabilidad en los resultados obtenidos.

Los modelos predictivos aplicados poseen una alta confiabilidad, retratado por la precisión total para las dos hipótesis (87.18% y 73.08%), así como el resultante $(R^2) de\ 0.996$ confirmando patrones que identifican cualitativamente.

Al evaluar con diferentes modelos las hipótesis, se logra identificar que la variable Departamento es influyente en ambas de diferentes maneras, sino es en el nivel y frecuencia de las capacitaciones que se dan, es con el nivel de conocimiento que se tienen sobre la gestión de activas de TI, por lo cual la estructura organizacional contribuye al desarrollo de conocimientos y la percepción sobre la eficiencia operativa. Lo que constituye una vulnerabilidad estructural, ya que áreas con menor capacitación presentan una mayor exposición a riesgos por desconocimiento o malas prácticas.

4.4.2 MODELOS APLICADOS

Para la Simulación de Escenarios Predictivos, se implementaron y compararon múltiples modelos, asegurando así la solidez de las conclusiones. La Figura 42 ilustra el flujo de trabajo en KNIME, debido a la limitación de la muestra (n = 41), se utilizó una técnica de aumento de datos (SMOTE) con fines exploratorios para identificar el peso predictivo de las variables como Formación en Ciberseguridad y eficiencia Operativa, en un escenario de big data.

Comenzamos con un modelo Random Forest utilizado para la Predicción de nivel de capacitación por departamento.

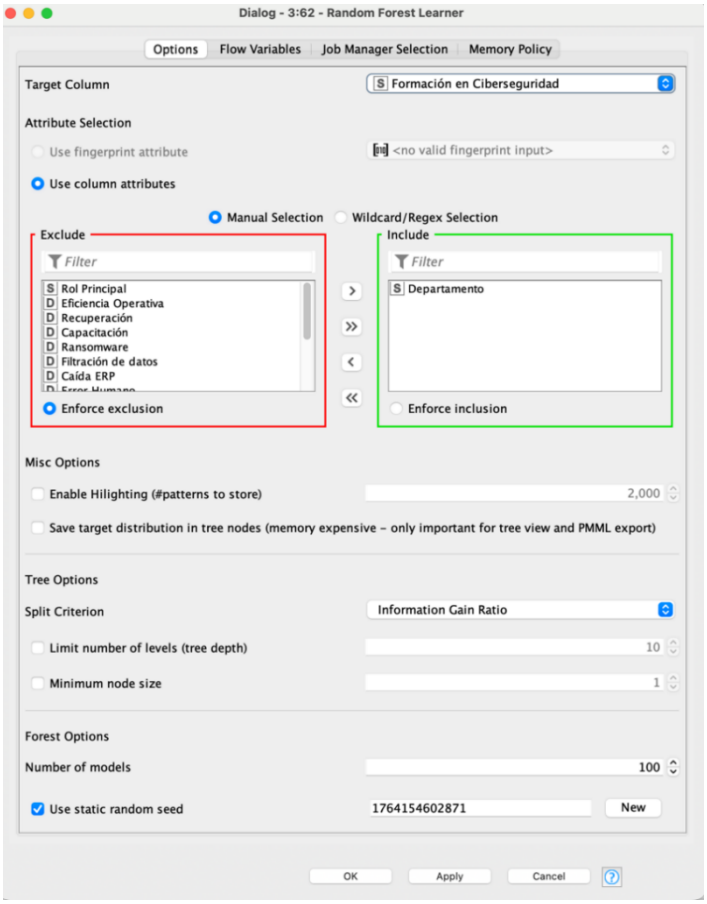


Figura 42. Configuración del Random Forest para la Predicción de nivel de capacitación por departamento

Fuente. Elaboración propia, software knime

La Tabla 31 presenta la Matriz de Confusión resultante del modelo de Random Forest. Esta matriz evidencia un excelente rendimiento predictivo, con una precisión global del 87.18%. El modelo mostró una capacidad particularmente alta para identificar correctamente la clase "Baja/Media" brecha de conocimiento, lo que refuerza la fiabilidad de las clasificaciones realizadas. El coeficiente Kappa de Cohen de 0.735 indica una concordancia sustancial entre las predicciones del modelo y los valores reales, muy por encima de lo que se esperaría por azar.

Tabla 31. Matriz de confusión aplicada al bosque aleatorio para la Predicción de nivel de capacitación por departamento

Matriz de Confusión

Confusion Matrix

	No, nunca. (Predicted)	No estoy seguro/a. (...	Sí, de forma regular ...	Sí, pero hace mucho...	
No, nunca. (Actual)	72	0	0	36	66.67%
No estoy seguro/a. (...	18	0	0	18	0.00%
Sí, de forma regular ...	18	0	36	18	50.00%
Sí, pero hace much...	18	0	0	234	92.86%
	57.14%	undefined	100.00%	76.47%	

Overall Statistics

Overall Accuracy	Overall Error	Cohen's kappa (κ)	Correctly Classified	Incorrectly Classified
73.08%	26.92%	0.531	342	126

Fuente. Elaboración propia, software knime

Complementariamente, se aplicó un modelo de Regresión Lineal para cuantificar la relación entre las variables. Los resultados en la Tabla 32 muestran los coeficientes del modelo, que permiten entender la magnitud y dirección del impacto de cada variable presentada.

Tabla 32. Regresión lineal aplicada a la Predicción de nivel de capacitación por departamento

Statistics on Linear Regression

Variable	Coeff.	Std. Err.	t-value	P>|t|
Departamento=Comercial	-0.1663	0.0497	-3.3486	0.0009
Departamento=Formación Médica	-0.9298	0.0932	-9.9803	0.0
Departamento=Gerencia	0.0702	0.0967	0.7263	0.4681
Departamento=Herramientas Digitales	-0.9298	0.0932	-9.9803	0.0
Departamento=Logística	0.0702	0.0825	0.8511	0.3953
Departamento=Operaciones	0.0702	0.0901	0.7796	0.4361
Departamento=Regencia y Calidad	0.0702	0.0664	1.0572	0.2911
Departamento=TI	0.0702	0.0848	0.8283	0.4081
Departamento=Visitas Médicas	-0.5801	0.0506	-11.4663	0.0
Intercept	4.9298	0.0266	185.0595	0.0

R-Squared: 0.4715
Adjusted R-Squared: 0.4584

Fuente. Elaboración propia, software knime

La Tabla 33, que contiene las métricas de evaluación del modelo de regresión (como el R^2 y el error cuadrático medio), confirma que el modelo tiene un alto poder explicativo para predecir la variable dependiente.

Tabla 33. Evaluación de modelo predictivo con la regresión lineal

R^2:	0.464
Mean absolute error:	0.18
Mean squared error:	0.1
Root mean squared error:	0.316
Mean signed difference:	-0.011
Mean absolute percentage error:	0.041
Adjusted R^2:	0.464

Fuente. Elaboración propia, software knime

4.4.2.1 VALIDACIÓN DE MODELOS Y CONTROL DE SESGO

Validación del modelo 1 – Random Forest para para la predicción de nivel de capacitación por departamento

Supuestos del modelo

- El conjunto de datos utilizado es representativo de la población objeto de estudio.
- Las variables independientes (departamento) contienen información relevante para explicar el comportamiento de la variable dependiente (Nivel de capacitación).
- La presencia de desbalance entre categorías no impide el aprendizaje del modelo, aunque puede afectar el desempeño en clases minoritarias.

Método de validación

La validación del modelo se realizó mediante la comparación entre los valores reales observados y las predicciones generadas por el modelo sobre un conjunto de validación independiente. Para este propósito se empleó una matriz de confusión, herramienta que permitió evaluar el desempeño del modelo tanto de forma global como por categoría específica.

Métricas de evaluación

- Exactitud global (Overall Accuracy): 73.08%
- El modelo clasificó correctamente 342 de un total de 468 observaciones, lo que refleja un desempeño general aceptable en el contexto de un problema de

clasificación multiclase.

- Error global (Overall Error): 26.92%. Indica que aproximadamente una cuarta parte de las observaciones fueron clasificadas de manera incorrecta.
- Coeficiente Kappa de Cohen ($\kappa = 0.531$). Este valor corresponde a un nivel de acuerdo moderado entre las clasificaciones reales y las predicciones del modelo, ajustando el efecto del acuerdo esperado por azar. Este resultado evidencia que el modelo logra capturar patrones relevantes presentes en los datos, aunque se acepta que puede ser mejorable.

Limitaciones del modelo

- La categoría "No estoy seguro/a" obtuvo una tasa de clasificación correcta del 0%, esto evidencia un desbalance de clases y presenta un bajo desempeño en categorías ambiguas o minoritarias.

Validación del modelo 2 – Regresión Lineal para para la predicción de nivel de capacitación por departamento

Supuestos del modelo

- Existe una relación lineal entre la variable dependiente (Nivel de capacitación) y la variable independiente (departamento).
- Este supuesto permite la aplicación del modelo para fines explicativos y predictivos, reconociendo que su incumplimiento puede afectar la precisión de los resultados.

Método de validación

- Se emplearon métricas de ajuste global y de error de predicción, propias de modelos de regresión.
- Adicionalmente, se evaluó la significancia estadística de los coeficientes estimados a través de pruebas t, lo que permitió identificar qué variables presentan una contribución estadísticamente significativa en la explicación de la variable dependiente.

Métricas de evaluación

- Coeficiente de determinación (R^2): 0.464 – 0.471. El modelo explica aproximadamente el 46% de la variabilidad total de la variable dependiente, lo que indica una capacidad explicativa moderada.
- R^2 ajustado: 0.458 – 0.464. El valor ajustado confirma que el nivel de explicación se mantiene estable al considerar el número de variables incluidas en el modelo.
- Diferencia media con signo (Mean Signed Difference): -0.011. El valor cercano a cero evidencias la ausencia de sesgo sistemático en las predicciones del modelo.

Limitaciones del modelo (con evidencia)

- Aunque el modelo explica aproximadamente el 46% de la variabilidad de la variable dependiente, existe un 54% no explicado, lo que evidencia la presencia de factores adicionales no incluidos en el modelo.
- Varios departamentos presentan coeficientes no estadísticamente significativos ($p > 0.05$), lo que indica que, para estos casos, no se puede afirmar una diferencia real respecto al departamento de referencia.

4.4.3 DISCUSIÓN DE HALLAZGOS

En base a los datos obtenidos por la evaluación de ambas hipótesis, es posible ir formando algunas ideas y temáticas principales; la brecha de conocimiento dentro de la organización **si existe**, pero no es homogénea.

Con una calificación promedio de 3.25/5 en las competencias ISO 27005, en donde se encontró que el **Establecimiento del Contexto** (2.9), tiene una menor calificación que el **Análisis de Riesgo** (3.6), se puede decir que los colaboradores pueden analizar riesgos existentes, pero no pueden identificar activos críticos del área de TI sistemáticamente y ser sujetos activos en el proceso de la seguridad de la información.

La cultura organizacional contribuye a la dependencia técnica; encontrando que un 85% de las respuestas en la pregunta "*¿Qué proceso seguiría en caso de detectar un virus dentro de los sistemas de la empresa (considere el ERP, el almacenamiento en la nube o las carpetas compartidas)? Detalle paso a paso su forma de evaluar el riesgo y las acciones que tomaría"* se

limitan a “contactar a TI”, contribuido a que el nivel del MTTR es alto, poseyendo un promedio de 346 horas para un ticket con prioridad alta, se entiende que la duración de los procesos y el poco conocimiento más allá de solicitar ayuda puede crear un cuello de botella que afecta la eficiencia operativa de la empresa y la percepción que los empleados tienen, así como sobrecargar el área de TI.

Si bien los empleados de la organización reconocen la importancia teórica de la gestión de riesgos en el área de TI, también carecen de herramientas para su implementación. Esto puede ser causado por una falta de capacitación frecuente y políticas de seguridad formalizadas.

4.4.4 LIMITACIONES

Se debe tomar en cuenta que, por la naturaleza y la brevedad del estudio de todo el fenómeno de investigación como tal, es posible que el desarrollo de algunas temáticas principales y la cantidad de datos recolectados con los instrumentos (en este caso, la encuesta estructurada) sea de una menor escala a lo esperado, pues existen factores a la hora de la recolección que no pueden ser controlados por los investigadores (por ejemplo, la falta de respuestas por parte de la muestra).

Sin embargo, para mitigar esta situación, se utilizaron técnicas de muestreo que requerían de una configuración bastante detallada y tomó algunas pruebas de error para evitar el sobremuestreo y el sesgo de clase que adquiere en algunos casos.

4.5 SÍNTESIS DE HALLAZGOS

4.5.1 PRINCIPALES HALLAZGOS

Se encontró que los modelos y métodos estadísticos que fueron utilizados son confiables para la prueba de la Hipótesis 2 y, por lo tanto, se puede decir que, si hay una relación entre la brecha de conocimiento, el departamento en que se labora y la consideración hacia la eficiencia operativa, fundamentado en un nivel confianza del 95% al haber hecho las pruebas.

Para la prueba de la Hipótesis 1, se encontró que si existe una diferencia significativa entre todos los departamentos al nivel de capacitación que se les da en cuanto a la gestión de activos de TI y buenas prácticas de uso, por lo cual se puede crear una vulnerabilidad para la organización.

Predomina una cultura de dependencia hacia el área de TI, evidenciada por respuestas cualitativas unidireccionales y elevados valores de MTTR. Esto señala un cuello de botella

operativo y una percepción de ineficiencia que afecta la resiliencia organizacional.

Se identificó una paradoja donde los colaboradores valoran teóricamente la ciberseguridad (puntuaciones 5/5 en importancia) pero carecen de las competencias prácticas para implementar controles básicos.

4.5.2 IMPLICACIONES

A nivel práctico, se considera que se podría enfocar los programas de capacitación hacia el ***establecimiento del contexto***, ya que se considera la competencia más débil. Sin embargo, considerando la variación entre el nivel de conocimiento y reforzamiento de capacitaciones dentro de los diferentes departamentos, no es viable un enfoque único para toda la organización.

Para mantener de manera continua la validación de que la brecha de conocimiento no se amplié, es adecuado un plan de evaluación periódica con el propósito de seguir midiendo el conocimiento.

A nivel organizacional, se infiere que la dependencia centralizada en TI es insostenible; para empezar a fomentar una cultura del buen uso y seguridad, es necesario concientizar a los empleados para trasladarse desde un enfoque reactivo a un preventivo, ya que una brecha de conocimiento representa el camino hacia un riesgo regulatorio.

Para la consideración de posibles investigaciones futuras en el ámbito farmacéutico, esta investigación puede establecer una línea base para comparativas entre el desarrollo del conocimiento y la gestión de riesgos para el área de TI, aunque el contexto del país posee factores culturales específicos de la región, la cultura organizacional como tema de estudio permite aplicar otras inferencias sobre como en la región existen ciertos atributos similares en cuanto a las brechas de conocimiento. De igual manera, puede servir de base para instrumentos de medición de conocimiento y capacitación específicos para empresas farmacéuticas latinoamericanas.

4.5.3 CONCLUSIONES PRELIMINARES

Existe una brecha de conocimiento significativa en gestión de riesgos de TI en Distribuidora Leterago, evidenciada por la falta de un modelo formal alineado con ISO 27005 y la ausencia de políticas documentadas.

El tiempo de respuesta a incidentes (MTTR) es elevado y variable, especialmente en tickets

de baja prioridad (hasta 1020.43 horas en promedio, como se puede ver en la figura), lo que refleja ineficiencia operativa y falta de procesos estandarizados. Se puede decir que la falta de conocimiento en gestión de riesgos se traduce en procesos reactivos, tiempos de respuesta prolongados (debido al MTTR alto distribuido entre los diferentes niveles de prioridad, como se puede ver en la figura 9) y mayor exposición a vulnerabilidades.

La ausencia de una cultura de seguridad se refleja en la poca prioridad que se da a la gestión de riesgos, la falta de políticas formales y el escaso involucramiento de la dirección, tomando en cuenta el nivel de la brecha de conocimiento, sería requerido un cambio estructural que integre la gestión de riesgos en la estrategia empresarial y fomente la responsabilidad compartida entre las áreas para formar un entorno integral con las herramientas que provee el área de TI.

La capacitación en ciberseguridad es insuficiente y desactualizada: de todos los encuestados, solo 3 personas (como es visto en la figura 16) reciben formación de formar regular y actualizada; el porcentaje restante declaran que no reciben de hace mucho tiempo o, en casos grave, nunca se ha hecho el acercamiento para su formación, creando una cultura organizacional que no prioriza la gestión de riesgos de TI, lo que se manifiesta en la falta de concientización, procedimientos reactivos y escaso apoyo de la alta dirección.

Los empleados no cuentan con herramientas ni procedimientos claros para identificar, reportar o mitigar riesgos, lo que impacta directamente en la productividad y continuidad del negocio.

La adopción de un marco como ISO 27005 no solo cerraría la brecha de conocimiento, sino que también mejoraría la gobernanza de TI y la resiliencia organizacional.

Se recomienda un enfoque de mejora continua, con revisiones periódicas, auditorías internas y ajustes basados en métricas y retroalimentación.

Los departamentos con mayor exposición a riesgos tecnológicos, pero que posee una concientización sobre la protección de datos y la importancia de eficiencia operativo, como es visto en las figuras 17 y 18; Logística y Finanzas se incluye dentro de estas áreas, tomando en cuenta la figura 11 y 12, ya que de igual manera presentan mayor volumen de incidentes, pero no necesariamente cuentan con mayor capacitación especializada. La formación es esporádica y no está alineada con las necesidades actuales de ciberseguridad, lo que perpetúa la brecha de

conocimiento y aumenta el riesgo operativo.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

En el siguiente capítulo, se desarrollarán las conclusiones que los investigadores han formulado como resultado del fundamento teórico (teorías de sustento, micro y macroentorno) siendo relacionado con el análisis exploratorio e inferencial de la información recolectada con los diferentes instrumentos y fuentes de datos. Asimismo, se espera que derivando de las conclusiones se puedan formular recomendaciones que permitan dar un panorama para atender y realizar acciones que contribuyan al desarrollo del fenómeno en estudio.

5.1 CONCLUSIONES

- La triangulación de datos cualitativos y cuantitativos orientado a responder la problemática sobre el diagnóstico de una brecha de conocimiento en los empleados de la filial en Honduras de Distribuidora Leterago, revela que, en efecto, **si** existe una brecha de conocimiento y esta afecta a los diferentes departamentos de la organización, así como ser un factor negativo de impacto en la percepción sobre la eficiencia operativa y exposición a vulnerabilidades. Como es mostrado en la **Tabla 24,** donde se muestra el promedio de calificaciones en diferentes aspectos sobre el conocimiento de gestión de riesgos para el área de TI, junto con el análisis de las respuestas cualitativas, demuestran que el nivel de competencia promedio se sitúa alrededor del 3**.29 puntos de posibles 5**, que si bien es una calificación considerada competente a un nivel básico, en el Establecimiento del Contexto se encuentra un promedio **menor a 2.9,** confirmando una brecha sustancial ante la medición contra un marco normativo. A esto se le suma una dependencia operacional hacia el área de TI bastante notable, teniendo en cuenta que el **85% de los encuestados** solamente se limitaron a responder ***"contactar a TI"*** ante la detección de un incidente sin tomar acciones preventivas.

- Al analizar el aspecto cualitativo de las encuestas, se encuentra que los factores organizacionales, como ser la **falta de formación** en ciberseguridad y la cultura vigente, que refleja un modo de operar **reactivo y no proactivo**, también perpetúan la brecha de conocimiento y debilitan la cultura de la seguridad informática. El **46.15% de los encuestados** indicaron que recibieron formación en ciberseguridad

"**hace mucho tiempo**", y el **23.08% nunca han recibido** capacitaciones relacionadas con el tema como lo sugiere la **Tabla 34**, significando que dos terceras partes de los encuestados no tienen las herramientas suficientes para poder tener una mentalidad proactiva hacia la respuesta a incidentes de índole informática; se revela un aprendizaje basado en el *bucle simple*, que también da paso a dar un límite en la cantidad y calidad de conocimiento que los empleados de la organización pueden transferirse entre sí. Los diferentes hallazgos también permiten dar peso a la Hipótesis Alternativa 1, donde se sugiere que el departamento y el nivel de capacitación que tienen los empleados de la Distribuidora Leterago influye en la importancia percibida que se la da a la gestión de riesgos para el área de TI.

- La exploración y análisis del rendimiento operativo, por medio del Reporte de Tickets y la extracción del MTTR (Tiempo Medio de Respuesta), permiten declarar que, aparte de generar ineficiencias sustanciales reflejadas por el tiempo que toma resolver un incidente, el proceso de atención a incidentes posee una variabilidad muy inestable; el análisis del MTTR, desglosado por medio del nivel de prioridad y sistema afectado, muestra que cuando un ticket posee una prioridad **baja** se resuelve en un tiempo promedio de **1020.43** horas, mientras que un ticket con prioridad alta tiene un promedio de **346 horas**, aproximadamente, **ver figura 9**. Si bien los tickets relacionados con la resolución y revisión de hardware toman **30 horas en promedio** de resolver, sistemas críticos, como el **AX Pharma 365** pueden tener incidencias que toman hasta **103 horas en promedio**, **ver figura 10**, reflejando que no existe una uniformidad en el proceso de atención y respuesta a incidentes en cualquier área o nivel de urgencia que se le debe dar. Esta variabilidad, sumada al patrón general de tiempos elevados, demuestra que la carencia de un proceso estructurado basado en normativas como ISO 27005 afecta directamente la capacidad del área de TI para identificar, priorizar y tratar amenazas, conectando así la brecha de conocimiento con el impacto que se tiene en la eficiencia operativa de la organización.

5.2 RECOMENDACIONES

- Se recomienda implementar un marco formal de gestión de riesgos basado en ISO 27005, acompañado de la estandarización de procedimientos y procesos de atención al usuario final, con el fin de reducir los altos tiempos de respuesta reflejados en el MTTR y mejorar la capacidad de prevención y contención de amenazas. La adopción del marco debe incluir evaluaciones periódicas que muestren la variabilidad operativa o su falta de esta. Al centrarse en los dominios que tienen un menor puntaje y, por tanto, mayor brecha, especialmente "Establecimiento del Contexto", que obtuvo 2.9/5, es posible hacer una transición adecuada hacia una organización que está en constante aprendizaje y apoyándose de programas que incluyan ejercicios de identificación de activos, análisis de amenazas y simulaciones de riesgo, el nivel de competencias puede aumentar de manera verificable en evaluaciones que hagan a posterior.
- Con el propósito de orientar la cultura organizacional hacia un aprendizaje de doble bucle, se recomienda diseñar e implementar un plan de capacitaciones que permita expandir los conocimientos de los dominios definidos por ISO 27005 con mayor brecha de conocimiento, así como un análisis de vulnerabilidades y riesgos por medio de la calculadora CVSS 4.0, la cual complementada con una matriz de riesgos asociados al área de TI como un todo y hacia los activos que esta posee, permitirá ir cerrando gradualmente la brecha de conocimiento, y también con el propósito de poder reducir la dependencia operacional que se tiene hacia el área de TI, así formando o educando los empleados para tener una mentalidad proactiva.
- Se recomienda formalizar y actualizar las políticas institucionales de seguridad de la información y respuesta a incidentes, integrando estas políticas a lo largo de todos los departamentos, con el propósito de reducir la dependencia técnica hacia el área de TI, reflejado por el 85% de respuestas del análisis cualitativo donde se plantea en únicamente acudir al área de TI para asistencia y soporte. La implementación debe contemplar una formación transversal, roles claros por departamento y mecanismos de reporte, que, agregando evaluaciones periódicas relacionadas con el plan de capacitaciones, sea una herramienta para asesorar y evaluar el nivel de conocimiento sobre la gestión de riesgos de TI en la

Distribuidora Leterago.

Tabla 34. Matriz relacional Objetivo → Resultado

Objetivo	Resultado	Conclusión	Entregable	Indicador
Diagnosticar la brecha de conocimiento en la gestión de riesgos de la seguridad de la información dentro del área de TI de Distribuidora Leterago para determinar su impacto en la exposición a vulnerabilidades y la eficiencia operativa, (M) mediante encuestas y análisis documental de reportes de incidentes, (R) para generar un diagnóstico base que informe futuras estrategias de mitigación, (T) durante el último trimestre de 2025.	Tabla 23, Tabla 24, Tabla 25, Figura 30	La triangulación de datos cualitativos y cuantitativos orientado a responder la problemática sobre el diagnóstico de una brecha de conocimiento en los empleados de la filial en Honduras de Distribuidora Leterago, revela que, en efecto, si existe una brecha de conocimiento y esta afecta a los diferentes departamentos de la organización, así como ser un factor negativo de impacto en la percepción sobre la eficiencia operativa y exposición a	Inventario y Clasificación de Activos de TI basado en ISO 27005	**Porcentaje de Activos Clasificados**

Objetivo	Resultado	Conclusión	Entregable	Indicador
		vulnerabilidades. Como es mostrado en la Tabla 24, donde se muestra el promedio de calificaciones en diferentes aspectos sobre el conocimiento de gestión de riesgos para el área de TI, junto con el análisis de las respuestas cualitativas, demuestran que el nivel de competencia promedio se sitúa alrededor del 3.29 puntos de posibles 5, que si bien es una calificación considerada competente a un nivel básico, en el Establecimiento del Contexto se encuentra un promedio menor a 2.9, confirmando una brecha		

Objetivo	Resultado	Conclusión	Entregable	Indicador
		sustancial ante la medición contra un marco normativo. A esto se le suma una dependencia operacional hacia el área de TI bastante notable, teniendo en cuenta que el 85% de los encuestados solamente se limitaron a responder "contactar a TI" ante la detección de un incidente sin tomar acciones preventivas.		
Determinar el nivel de eficiencia operativa por medio de la respuesta a incidentes, (M) analizando el Tiempo Medio de Respuesta (MTTR) de los (A) incidentes reportados en los	Tabla 13, Tabla 14, Figura 8, Figura 9	La exploración y análisis del rendimiento operativo, por medio del Reporte de Tickets y la extracción del MTTR (Tiempo Medio de Respuesta), permiten declarar que, aparte de	Matriz de Evaluación de Riesgos basada en ISO 27005.	**MTTR**

Objetivo	Resultado	Conclusión	Entregable	Indicador
últimos 12 meses, (R) para conectar la brecha de conocimiento con resultados operativos, (T) en un plazo de ocho semanas.		generar ineficiencias sustanciales reflejadas por el tiempo que toma resolver un incidente, el proceso de atención a incidentes posee una variabilidad muy inestable; el análisis del MTTR, desglosado por medio del nivel de prioridad y sistema afectado, muestra que cuando un ticket posee una prioridad baja se resuelve en un tiempo promedio de 1020.43 horas, mientras que un ticket con prioridad alta tiene un promedio de 346 horas, aproximadamente. Si bien los tickets		

Objetivo	Resultado	Conclusión	Entregable	Indicador
		relacionados con la resolución y revisión de hardware toman 30 horas en promedio de resolver, sistemas críticos, como el AX Pharma 365 pueden tener incidencias que toman hasta 103 horas en promedio, reflejando que no existe una uniformidad en el proceso de atención y respuesta a incidentes en cualquier área o nivel de urgencia que se le debe dar. Esta variabilidad, sumada al patrón general de tiempos elevados, demuestra que la carencia de un proceso estructurado		

Objetivo	Resultado	Conclusión	Entregable	Indicador
		basado en normativas como ISO 27005 afecta directamente la capacidad del área de TI para identificar, priorizar y tratar amenazas, conectando así la brecha de conocimiento con el impacto que se tiene en la eficiencia operativa de la organización.		
Identificar los factores organizacionales que perpetúan la brecha de conocimiento, (M) mediante el análisis de la documentación de políticas y (A) encuestas con los líderes de equipo, (R) para comprender las causas raíz	Tabla 23, Tabla 30	Al analizar el aspecto cualitativo de las encuestas, se encuentra que los factores organizacionales, como ser la falta de formación en ciberseguridad y la cultura vigente, que refleja un modo de operar reactivo y no proactivo, también perpetúan la	Plan de Capacitación en Gestión de Riesgos de la Seguridad de la Información	**Calificaciones de personal capacitado**

Objetivo	Resultado	Conclusión	Entregable	Indicador
culturales, (T) en un plazo de seis semanas. Determinar el nivel de conocimiento sobre gestión de riesgos de seguridad de la información en el personal de TI, (M) utilizando una matriz de competencias basada en ISO 27005 y (A) encuestas a todo el personal del área, (R) para cuantificar la brecha de habilidades, (T) en un plazo de cinco semanas.		brecha de conocimiento y debilitan la cultura de la seguridad informática. El 46.15% de los encuestados indicaron que recibieron formación en ciberseguridad "hace mucho tiempo", y el 23.08% nunca han recibido capacitaciones relacionadas con el tema, significando que dos terceras partes de los encuestados no tienen las herramientas suficientes para poder tener una mentalidad proactiva hacia la respuesta a incidentes de índole informática; se revela un		

Objetivo	Resultado	Conclusión	Entregable	Indicador
		aprendizaje basado en el bucle simple, que también da paso a dar un límite en la cantidad y calidad de conocimiento que los empleados de la organización pueden transferirse entre sí. Los diferentes hallazgos también permiten dar peso a la Hipótesis Alternativa 1, donde se sugiere que el departamento y el nivel de capacitación que tienen los empleados de la Distribuidora Leterago influye en la importancia percibida que se la da a la gestión de riesgos para el área de TI.		

Fuente. Elaboración Propia

CAPÍTULO VI. APLICABILIDAD

El siguiente capítulo tiene como propósito desarrollar una propuesta de aplicabilidad para la filial en Honduras de Distribuidora Leterago en base a los hallazgos obtenidos de la investigación.

La propuesta responde a la necesidad de reducir los tiempos de respuesta durante el manejo de incidentes, tratar la brecha de conocimiento en las diferentes áreas de la organización y mejorar la eficiencia operativa del área de TI, de esta manera asegurando la continuidad de las operaciones para un rubro tan exigente como la distribución de productos farmacéuticos.

6.1 NOMBRE DE LA PROPUESTA

Modelo Integral de Gestión de Riesgos para el área de TI basado en normativa ISO 27005 y CVSS 4.0 para Distribuidora Leterago en Honduras.

6.2 JUSTIFICACIÓN DE LA PROPUESTA

Los hallazgos de la investigación demostraron que en la filial de Honduras de la Distribuidora Leterago existe una brecha significativa de conocimiento técnico sobre la gestión de riesgos de TI dentro de los empleados de las diferentes áreas; al carecer de un modelo formal de gestión de riesgos alineado con estándares internacionales, como ser la ISO 27005, no existe un método unificado para identificar y tratar incidentes, por lo cual se derivan riesgos y vulnerabilidades que pueden afectar la disponibilidad del negocio, la integridad y confidencialidad en los datos que poseen los activos del área de TI.

De igual manera, tener tiempos de respuesta prolongados durante el manejo de incidentes de todo tipo de prioridad, que se ve reflejado en el MTTR, comprometen la eficiencia operativa. Desde el marco teórico, la ISO 27005 proporciona directrices para la identificación, evaluación y tratamiento de riesgos asociados al área de TI, mientras que CVSS 4.0 provee un método cuantificable para medir la severidad de vulnerabilidades con métricas estandarizadas y comparables.

De acuerdo con la Teoría del Aprendizaje Organizacional, como se logra inferir en base a lo planteado por (Fiol & Lyles, 1985), el aprendizaje avanzado o de bucle doble es aquel que apunta a crear nuevas reglas que no se limiten a un universo definido anteriormente; por lo tanto,

se espera que, con la implementación de este modelo, exista un cambio positivo en la cultura organizacional ante la percepción sobre el área de TI y la forma en la que los usuarios interactúen con ella.

Asimismo, se espera que el área de TI pueda tener una mejora en su capacidad de respuesta ante incidentes de todo tipo de prioridad, de esta manera disminuyendo el MTTR.

6.3 ALCANCE DE LA PROPUESTA

El alcance de esta propuesta se limita hacia su aplicación dentro de la filial hondureña de Distribuidora Leterago, en donde se coordinará entre el área de TI apuntando hacia los diferentes empleados del área administrativa de la organización. Es posible definir la propuesta definiendo los siguientes objetivos:

- **Implementar**, dentro de un periodo máximo de 12 meses, un modelo integral de gestión de riesgos para el área de TI, que incorpore instrumentos de medición y monitoreo, utilizando normativas como ISO 27005, con el fin de fortalecer el nivel de gobernanza institucional y asegurando su cumplimiento mediante la aplicación de indicadores de desempeño definidos previamente.
- **Documentar y clasificar** los activos de TI, la elaboración de una matriz de riesgos de TI y la priorización de vulnerabilidades con el propósito de disminuir el MTTR dentro de un periodo máximo de 9 meses.
- **Implementar**, durante un periodo máximo de 9 meses, un plan de capacitación dirigido al personal administrativo, logrando una cobertura mínima del 80% del personal involucrado, con el propósito de disminuir la dependencia actual hacia el área de TI para las operaciones diarias y orientando a un cambio positivo de la cultura organizacional.

6.4 DESCRIPCIÓN Y DESARROLLO

6.4.1 DESCRIPCIÓN

La siguiente propuesta consiste en diseñar e implementar un **Modelo Integral de Gestión de Riesgos para el área de TI**, que se compone de dos eslabones principales:

- **Evaluación y Priorización de Riesgos y Vulnerabilidades** utilizando CVSS 4.0

y matrices de evaluación ISO 27005.

- **Capacitación y fortalecimiento de competencias del personal administrativo y de TI** en análisis de riesgos y evaluación de vulnerabilidades.

6.4.2 DESARROLLO

Para poder materializar la idea de un modelo de gestión de riesgos de TI, es necesario plasmar diferentes documentos, proyectos o sistemas que den las condiciones para cumplir los objetivos definidos; en este caso, se definirán 4 entregables que corresponden a los 2 eslabones principales por los que se plantea fundamentar el modelo integral.

- *Entregable 1:* **Inventario y Clasificación de Activos de TI basado en ISO 27005.**

  Se plantea realizar un registro y clasificación completa de todos los activos de la organización en la filial de Honduras, la cual consistirá en una descripción detallada del activo, así como su clasificación por dos criterios importantes: el **tipo de activo** y **el nivel de criticidad.**

  El **tipo de activo** representa una categorización por su estado tangible; se considera físico todo aquello como hardware que tiene un espacio dentro de las oficinas de la organización, como ser servidores, computadoras, tablets, componentes como memorias RAM o cables de red y centros de datos, mientras que un activo virtual es todo aquello que existe dentro del entorno tecnológico de la empresa y se interactúa con él por medio del uso de hardware, como ser licencias para programas y sistemas operativos, centros de administración de servicios de TI y sistemas y aplicaciones que utiliza la organización.

  Se realizará una evaluación de dependencias del activo en los procesos del área, lo que significa que se realizará una enumeración de todos los procesos del área de TI en los que se ve involucrado ese activo, información que será de uso necesario para poder dar un nivel de criticidad al tener un mejor contexto de cómo se utiliza ese activo en la empresa y cuál es el propósito que se le ha dado, así como evaluar el impacto que puede tener en caso del fallo en sus funciones.

  El nivel de criticidad se puede dar en 3 categorías: **bajo, medio y alto**. Cuando un activo tiene una baja criticidad, implica que el activo no presenta un mayor riesgo

o amenaza en caso de ocurrir un desperfecto o falla imprevista y la organización puede operar sin ningún inconveniente ante la ausencia de este activo; si a un activo se le clasifica con un nivel de criticidad media, significa que la organización puede tener inconvenientes menores pero notables ante la ausencia de este activo, significando que la eficiencia operativa se verá afectada e incluso puede provocar atrasos en sus operaciones diarias. Por último, un activo es de criticidad alta si una falla, desperfecto o pérdida de información dentro de sí implica una falla en sus operaciones diarias, siendo posible hasta la paralización de un proceso por la ausencia de este activo, considerado casi indispensable.

El propósito de realizar estas tareas es poder darle un mejor contexto a los encargados del área de TI sobre los activos que poseen y la valoración que se les debe dar a la hora de uso; proveer contexto sobre la importancia de un activo es esencial para entender la importancia con la que se debe enseñar hacia afuera del área al usuario final.

El entregable será un archivo de Excel que contenga todos los activos del área de TI clasificados con los criterios anteriormente mencionados.

Tabla 35. Tabla por utilizar para la medición de la criticidad de los activos del área de TI.

Nombre del Activo	Descripción del Activo	Tipo de Activo	Nivel de Criticidad	Dependencias del Activo en procesos del área
Nombre detallado del Activo		*Físico (Hardware), Virtual (Software)*	*Bajo, Medio, Alto*	*Enumeración de los procesos de los que se depende para este activo*

Fuente: Elaboración Propia

- *Entregable 2:* **Matriz de Evaluación de Riesgos basada en ISO 27005.**

  Como segundo entregable, se plantea realizar una matriz de evaluación de riesgos relacionados con los activos anteriormente clasificados y entregados en el Entregable 1, por lo que será de gran importancia primero realizar el Inventario y Clasificación de Activos.

  La matriz de evaluación de riesgos empieza por la identificación de elementos como el **tipo** de riesgo, en donde se utiliza el Entregable 1 para relacionar el riesgo

de cada uno de los activos por su tipo (físico, virtual) o si este riesgo conlleva a lo logístico. Se continúa por la **identificación** del riesgo, posteriormente realizando el **análisis**, que conlleva detectar cuales pueden ser las consecuencias de la omisión de este riesgo sobre la organización.

Para poder valorar cuantitativamente todos los riesgos y de esta manera, proveer las herramientas necesarias para poder asegurar no solo la gestión de riesgos dentro del área de TI, sino contribuir a la socialización del conocimiento dentro de la organización, se utilizan las escalas de medición mostradas en la Tabla 35, la cual especifica que en base a la multiplicación de la categoría de **Probabilidad** contra el **Impacto** se obtiene el **Nivel de Urgencia,** que permite priorizar y clasificar los riesgos.

El resultado de esta tarea se verá reflejada en un archivo de Excel que contenga todos los riesgos clasificados y calificados basándose en la Tabla 36.

Tabla 36. Escalas de medición del nivel de urgencia para la gestión de riesgos del área de TI

ESCALA (PROBABILIDAD):	ESCALA (IMPACTO):	NIVEL DE URGENCIA:
5: Con Certeza	5: CATASTRÓFICO	20-25: EXTREMO
4: Muy Probable	4: MAYOR	15: MUY ALTO
3: Media	3: MEDIO	10-12: ALTO
2: Baja	2: BAJO	5 - 9: MEDIO
1: Improbable	1: INSIGNIFICANTE	3-4: BAJO
		1 - 2: MUY BAJO

Fuente. Elaboración propia, información obtenida de la normativa ISO 27005

Tabla 37. Formulario para la identificación de cada uno de los riesgos del área de TI.

TIPO DE RIESGO	IDENTIFICACIÓN DEL RIESGO	ANÁLISIS DEL RIESGO	PROBABAILIDAD	IMPACTO	VALOR	NIVEL DE URGENCIA
Lógico, Físico (Hardware), Virtual (Software)			Escala de 1 - 5	Escala de 1 - 5	(Probabilidad) x (Impacto)	1 - 25

Fuente: Elaboración Propia

- *Entregable 3:* **Sistema de Priorización de Vulnerabilidades utilizando CVSS 4.0.**

  Se plantea utilizar la calculadora de vulnerabilidades CVSS en su versión 4.0 para realizar la valoración de vulnerabilidades que se deriven de los activos virtuales y físicos de la organización; considerando que esta calculadora solo está disponible en línea, el entregable se dará en un documento PDF enumerando todas las vulnerabilidades que hayan sido identificadas, adherido del activo del que provienen.

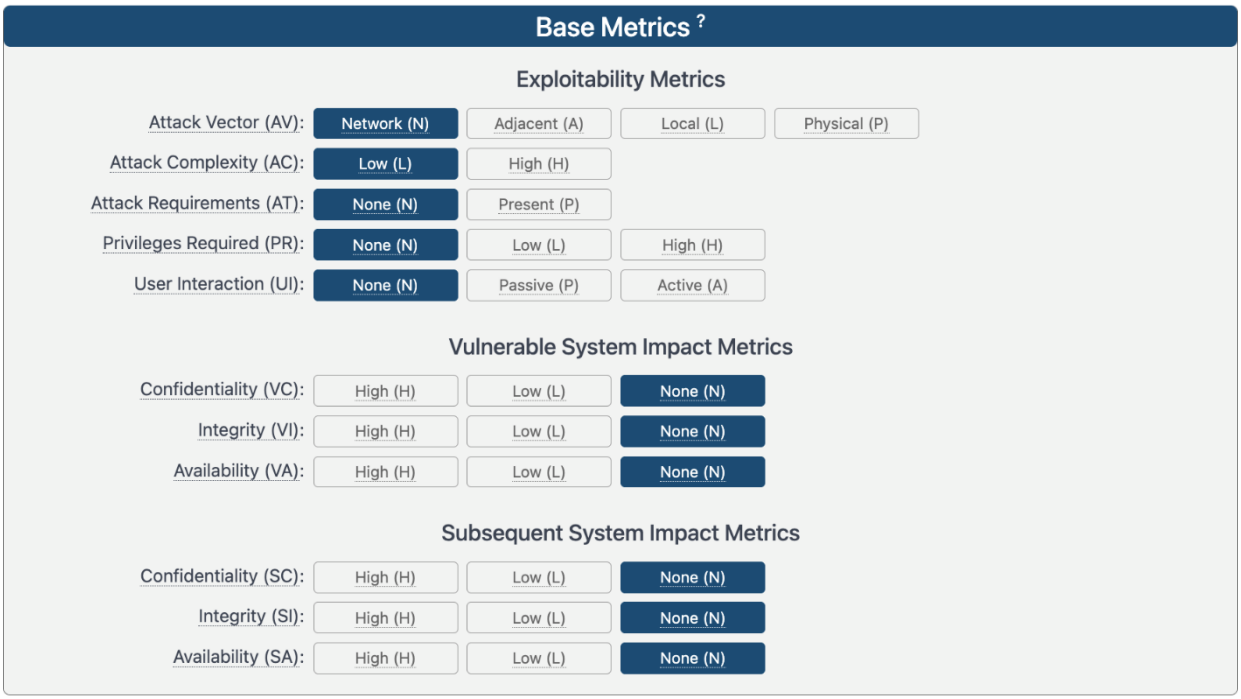
  Esta calculadora automatiza el cálculo de métricas que el evaluador ingresa, traduciendo métricas cualitativas en una escala numérica con rango de 0 a 10 puntos, donde:

  - De 0.1 a 3.9 se considera como **Bajo**.
  - De 4.0 a 6.9 puntos se considera como **Medio.**
  - De 7.0 a 8.9 se considera como **Alto**.
  - De 9.0 a 10 se considera como **Crítico.**

  CVSS 4.0 tiene 4 grupos de métricas donde se debe ingresar la información, siempre teniendo en cuenta el contexto empresarial. Cada métrica posee un macroelemento compuesto de diferentes elementos que forman parte de la calificación de cada uno de ellos, posteriormente siendo una característica con su propia puntuación.

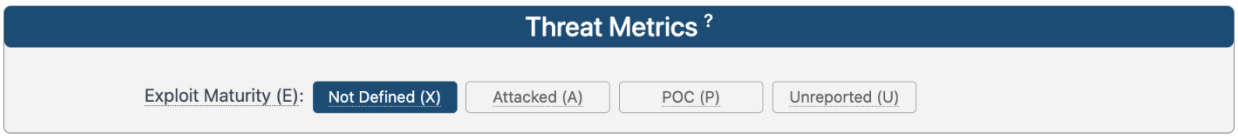
  La **Métrica Base** evalúa características intrínsecas de la vulnerabilidad encontrada. Con macroelementos como la Explotabilidad, que evalúa el contexto requerido para activar la vulnerabilidad, el Impacto en las Métricas de Seguridad, que evalúa como afecta en la puntuación de KPIs definidos y orientados a la ciberseguridad, y Requisitos de Seguridad posteriores a la Explotación, la Métrica Base provee la identificación del contexto de la vulnerabilidad.

Figura 43: Métricas Base para la evaluación de vulnerabilidades en la calculadora CVSS 4.0



La **Métrica de Amenaza** evalúa el estado actual de la posibilidad de explotación en el mundo, midiendo la Probabilidad.

Figura 44: Métricas de Amenaza para la evaluación de vulnerabilidades en la calculadora CVSS 4.0

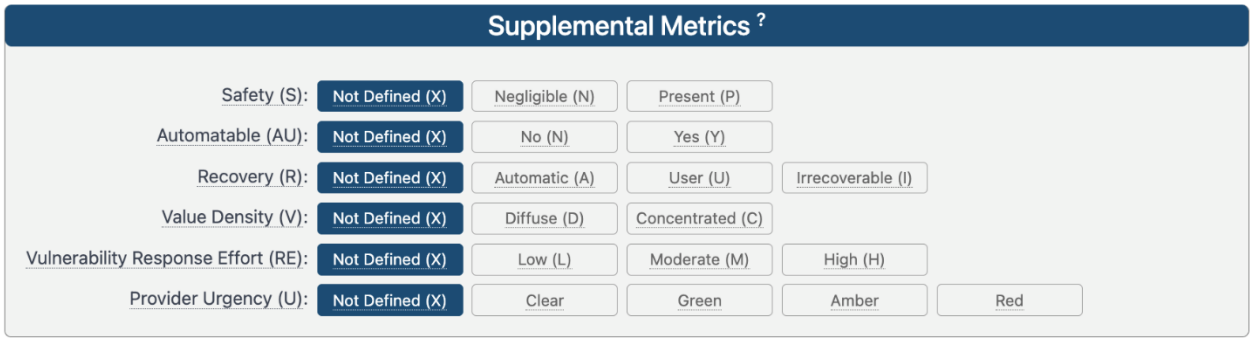


La **Métrica Ambiental** permite ajustar la puntuación total de la evaluación según el entorno específico de la organización, en donde los macroelementos evalúan el nivel de manejo que la organización puede tener (dentro de Control de Seguridad Mitigante) y qué impacto puede tener en su misión y propósito (considerado dentro de Impacto en la Misión/Propósito).

Figura 45: Métricas Ambientales para la evaluación de vulnerabilidades en la calculadora CVSS 4.0

La **Métrica Suplemental** es una sección que permite dar contexto para la gestión correcta de la vulnerabilidad, donde se especifican elementos que permiten dar condiciones para la creación de soluciones o procedimientos ante lo que podría afectar la vulnerabilidad dentro de la seguridad de la organización.

Figura 46: Métricas Suplementales para la evaluación de vulnerabilidades en la calculadora CVSS 4.0



- *Entregable 4:* **Plan de Capacitación en Gestión de Riesgos de TI.**

  Como último entregable y, con el propósito de ser un aporte para todos los departamentos de la organización, es la creación de un plan de capacitación orientado a la gestión de riesgos tecnológicos para las tecnologías que maneja el área de TI dirigida a los usuarios finales, en este caso, los empleados de Distribuidora Leterago.

  Se plantea la creación de material didáctico ilustrado en diferentes presentaciones que permitan transferir el conocimiento necesario para poder identificar riesgos, amenazas y dar las herramientas necesarias para el buen uso de la tecnología en el área de trabajo.

  Se compondrá de 3 módulos principales que abarcan de manera general los temas relacionados con la gestión de riesgos de TI, como ser el **Manejo de Incidentes**, la **Identificación de Vulnerabilidades** y **Contenido Malicioso**, y la socialización y concientización de la **Cultura de Seguridad Organizacional.** Los módulos se deberán estructurar para que su enseñanza abarque 16 horas por módulo, realizando una estimación pedagógica, las cuales pueden ser distribuidas por 2 horas a la semana, por 2 meses, con el propósito de sintetizar los conocimientos de una manera que sea digerible para personas que no tienen el mismo conocimiento técnico de los empleados que laboran en el área de TI, así como poder dar lugar a la enseñanza de temas que vayan dando un recorrido específico por cada tema principal del módulo manteniendo un dinamismo que retenga el interés de los usuarios finales.

  Con el propósito de velar por la implementación correcta y posibilidades de mejora continua de los programas de capacitación, se formularán evaluaciones que puedan medir los conocimientos adquiridos de esta capacitación, orientado a los empleados de Distribuidora Leterago. Las evaluaciones se deberán hacer al final de la enseñanza de cada módulo.

  El resultado de este entregable se verá reflejado no solamente en las diapositivas que se creen para la socialización de los temas, sino un archivo de Microsoft Word detallando los temas a discutir, cronograma de actividades de enseñanza y

estructuración de pruebas de conocimiento.

La siguiente tabla tiene como propósito mostrar de manera sintetizada el contenido de cada uno de los entregables, como ser el contenido del entregable, una breve descripción del proceso y su resultado esperado.

Tabla 38. Entregables del Modelo Integral / Fases del proyecto

Entregable	**Contenido del entregable**	**Resultado Esperado**
Inventario y Clasificación de Activos de TI basado en ISO 27005.	Plantilla de identificación de activos físicos, lógicos y de información. Valoración por nivel de criticidad (Baja, Media, Alta) Dependencias del activo dentro de los procesos del área.	Archivo de Microsoft Excel que contiene una colección de datos representando los activos del área de TI. Se puede aplicar CVSS 4.0 para los riesgos asociados
Matriz de Evaluación de Riesgos basada en ISO 27005.	Identificación de amenazas (naturales, técnicas, humanas). Identificación de probabilidad e impacto del riesgo (utilizando una escala del 1 al 5) Planteamiento de nivel de riesgo y decisión (se puede catalogar como *Aceptar, Mitigar, Transferir, Evitar*).	Mapa de riesgos alineado a criterios de la norma ISO 27005.

Entregable	Contenido del entregable	Resultado Esperado
Sistema de Priorización de Vulnerabilidades utilizando CVSS 4.0.	Evaluación del activo del área de TI utilizando la calculadora CVSS 4.0, tomando como resultado y clasificación el puntaje asignado (con rango de 0 -10, donde se considera Bajo de 0.1 a 3.9, Medio de 4.0 a 6.9, Alto de 7.0 a 8.9 y Crítico de 9.0 a 10).	Priorización objetiva y estandarizada del tratamiento de vulnerabilidades.
Plan de Capacitación en Gestión de Riesgos de Seguridad de la Información en.	Sílabos y contenido didáctico para cada módulo: Manejo de incidentes, Identificación de vulnerabilidades y contenido malicioso, Fomentar cultura de seguridad organizacional. Pruebas de conocimiento basadas en el contenido didáctico.	Material visual para realizar las capacitaciones dirigidas al personal administrativo.

Fuente. Elaboración propia

6.5 MEDIDAS DE CONTROL

Para poder medir la efectividad de un proyecto y definir su viabilidad, es necesario detallar indicadores que permitan visualizar el progreso de cada etapa y transmitir a un resultado tangible el nivel de calidad de los entregables y su implementación. La presentación de estos indicadores se realizará por medio de un tablero de visualización en Power BI, donde se estará utilizando como origen de los datos los diferentes archivos o reportes que correspondan a cada indicador. Por ejemplo, el porcentaje de activos clasificados se extraerá del inventario y clasificación de los activos de TI, el MTTR se extrae del Reporte de Tickets, como fue mostrado en la sección 4.1.1,

y las calificaciones de personal capacitado se extraerán del resultado de todas las evaluaciones realizadas por módulo.

Para entrar en detalle, los indicadores serán el **Porcentaje de Activos Clasificados**, el **MTTR** (Tiempo Promedio de Respuesta) y las **Calificaciones de Personal Capacitado**.

- **Porcentaje de Activos Clasificados**
    - **Definición**

      Se considera como el nivel de avance en la categorización del inventario completo de la filial hondureña de la empresa, en base al total de activos que el área posee. Se toma en cuenta como categorizado cuando ya se ha calculado su criticidad y categorización como activo físico o virtual, así como su dependencia en los procesos del área de TI. Se realizará con una frecuencia mensual.

    - **Fórmula**

      Contabilización del avance del entregable contra el total de activos existentes.

      (Activos Contabilizados / Total de Activos)

    - **Fuente de datos**

      Entregable 1: Inventario y Clasificación de Activos de TI basado en ISO 27005.

    - **Responsable**

      Jefatura de TI.

- **MTTR**
    - **Definición**

      Tiempo promedio en el que los encargados del manejo del Sistema de Tickets responden y actúan ante una incidencia que es reportada por un usuario final de la organización. La medición se realizará con una frecuencia mensual. Actualmente es de un total de 391.31 horas.

- **Fórmula**

  Se realiza una sumatoria de todos los tiempos de respuesta de los incidentes ocurridos dentro del periodo de tiempo establecido, en este caso, cada mes, y se divide entre la cantidad total de incidentes que ocurrieron en este intervalo.

  (Σ Tiempos de Respuesta / Cantidad Total de Incidentes)

- **Fuente de datos**

  Reporte de Tickets del Sistema manejado por la organización.

- **Responsable**

  Encargado de TI.

- **Calificaciones del Personal Capacitado**
  - **Definición**

    El promedio del resultado de las evaluaciones impartidas por la organización hacia los empleados de esta, basados en el material didáctico de la capacitación, divididos por cada uno de los módulos planificados.

  - **Fórmula**

    Se realiza una sumatoria de todas las calificaciones obtenidas de la evaluación y se divide por la cantidad total de evaluaciones realizadas de cada uno de los módulos.

    (Σ Calificaciones obtenidas/ Cantidad Total de Evaluaciones Realizadas)

  - **Fuente de datos**

    Reporte digitalizado de las calificaciones obtenidas por cada módulo de capacitación.

  - **Responsable**

    Jefatura de TI y Jefatura de Recursos Humanos.

Tabla 39. Indicadores de cumplimiento del proyecto

Indicador	Descripción	Fórmula	Frecuencia	Límite Aceptable
Porcentaje de activos clasificados	Nivel de avance del inventario y activos que ya han sido clasificados	Activos clasificados / Total de Activos	Mensual	80% de todos los activos como mínimo, el 100% de los activos como máximo.
MTTR	Tiempo promedio de respuesta a los incidentes ingresados en la Plataforma de Tickets	Sumatoria de Tiempos de Respuesta / Cantidad de Incidentes	Mensual	Reducción de al menos un 50% del promedio del MTTR actual.
Calificaciones de personal capacitado	Evaluaciones del contenido proveniente de las capacitaciones	Calificación promedio de cada prueba de los módulos	A la finalización de cada módulo	85% de calificación como mínimo de aprobación, 100% como máximo.

Fuente. Elaboración propia

Con el propósito de sintetizar y resumir el hilo conductivo de la investigación, se realiza la siguiente tabla que mostrará la manera en la que cada uno de los Objetivos planteados en el Capítulo 1 revelan resultados importantes que permiten generar conclusiones verificables basadas en datos recolectados que tienen un método de validación de acorde con el modelo, que por última instancia, llevan a los investigadores a crear la propuesta actual, donde existe un entregable y un indicador correspondiente.

6.6 CRONOGRAMA DE IMPLEMENTACIÓN Y PRESUPUESTO

La siguiente sección tiene como propósito definir la lista de actividades a realizar para la implementación del modelo integral de gestión de riesgos de TI, así como los responsables de ejecutar cada una de las actividades con su respectivo tiempo de duración; tomando en cuenta que para obtener el tiempo y costo monetario se realiza una estimación, se utilizará la técnica PERT, que consiste en tomar 3 valores para poder crear escenarios donde se considere el escenario más probable (MP), el escenario optimista (O) y el escenario pesimista (P). En este caso, la **distribución beta** es la decisión más prudente, considerando que puede ser un proyecto con alta incertidumbre.

6.6.1 CRONOGRAMA DE IMPLEMENTACIÓN

Tabla 40. Cálculo de valores PERT

Fase	Actividad	Tiempo MP	Tiempo O	Tiempo P	Duración Estimada (O+4MP+P) /6	Responsable
Fase 1: Diagnóstico Inicial	Levantamiento de activos	*2 semanas*	*1 semana*	*3 semanas*	*2 semanas*	Jefatura TI, Encargado de TI
	Evaluación preliminar de riesgos	*1 semana*	*5 días*	*2 semanas*	*1 semana + 1 día*	Encargado de TI
Fase 2: Diseño de Modelo Integral	Desarrollo de matriz de evaluación de riesgos basada en ISO 27005	*1 mes*	*2 semanas*	*2 meses*	*1 mes + 2.5 días*	Jefatura TI, Encargado de TI
	Desarrollo de Sistema de Priorización de Vulnerabilidades	*2 meses*	*1 mes*	*2 meses y medio*	*1 mes + 25.5 días*	
	Desarrollo de Plan de Capacitación	*1 mes*	*3 semanas*	*1 mes y medio*	*1 mes + 1 día*	
Fase 3: Presentación y Evaluación del Modelo	Presentación de Matriz de Evaluación de Riesgos y Sistema de Priorización de Vulnerabilidades	*2 días*	*1 día*	*3 días*	*2 días*	Jefatura TI, Encargado de TI, Encargados de Recursos Humanos
	Presentación del Plan de Capacitación	*1 día*	*1 día*	*2 días*	*1.5 días*	
	Ajustes al modelo en base a retroalimentación	*3 semanas*	*2 semana*	*1 mes*	*21 días*	Jefatura TI, Encargado de TI
Fase 4: Implementació	Implementación de gestión de	*2 semana*	*1 semana*	*3 semana*	*2 semanas*	Encargado de TI,

Fase	Actividad	Tiempo MP	Tiempo O	Tiempo P	Duración Estimada (O+4MP+P) /6	Responsable
n del Modelo	riesgos y consideración de vulnerabilidades hacia los procesos, activos y operaciones de TI.	*s*		*s*		Encargados de Recursos Humanos
Fase 5: Capacitación	Módulo 1	*2 meses*	*1 mes y medio*	*2 meses y medio*	*2 meses*	Encargado de TI, Encargados de Recursos Humanos
	Evaluación del Módulo 1	*2 días*	*1 día*	*3 días*	*2 días*	
	Módulo 2	*2 meses*	*1 mes y medio*	*2 meses y medio*	*2 meses*	
	Evaluación del Módulo 2	*2 días*	*1 día*	*3 días*	*2 días*	
	Módulo 3	*2 meses*	*1 mes y medio*	*2 meses y medio*	*2 meses*	
	Evaluación del Módulo 3	*2 días*	*1 día*	*3 días*	*2 días*	
Fase 6: Evaluación	Evaluación de indicadores de desempeño	*3 días*	*1 día*	*4 días*	*3 días*	Jefatura TI, Gerencia General

Fuente: Elaboración propia

6.6.2 PRESUPUESTO

Tabla 41. Presupuesto estimado por cada fase del proyecto.

Presupuesto estimado por fase del proyecto					
Fase del Proyecto	**Concepto de Costo**	**Descripción del Recurso**	**Cantidad / Duración**	**Costo Unitario (HNL)**	**Costo Total (HNL)**
Fase 1: Diagnóstico Inicial	Recursos humanos	Jefatura TI (levantamiento de activos)	2 semanas	15000 (salario quincenal)	15000

Presupuesto estimado por fase del proyecto					
	Recursos humanos	Encargado TI (evaluación preliminar de riesgos)	1 semana	9000 (salario quincenal)	4500
	Materiales	Formularios, plantillas, documentación técnica	2 licencias anuales	7692	7692
	Subtotal Fase 1				**34884**
Fase 2: Diseño del Modelo Integral	Recursos humanos	Jefatura TI (matriz ISO 27005)	1 mes	15000 (salario quincenal)	30000
	Recursos humanos	Encargado TI (Calculo de CVSS 4.0)	2 meses	9000 (salario quincenal)	36000
	Tecnología	Software de hojas de cálculo avanzadas (Suite de Microsoft)	Licencia anual	7692	0 (incluido en la Fase 1)
	Subtotal Fase 2				**66000**
Fase 3: Presentación y Evaluación	Recursos humanos	Equipo TI (presentación técnica)	3 días	0	0
	Recursos humanos	Ajustes al modelo (jefatura y encargado)	3 semanas	15000 (salario quincenal de Jefatura) + 9000 (salario quincenal del Encargado)	36000
	Materiales	Documentación ejecutiva e informes (suite de Microsoft)	Licencia anual	7692	0 (incluido en la Fase 1)

Presupuesto estimado por fase del proyecto					
	Subtotal Fase 3				**36000**
Fase 4: Implementación del Modelo	Recursos humanos	Equipo TI (jefatura y encargado)	2 semanas	15000 (salario quincenal de Jefatura) + 9000 (salario quincenal del Encargado)	24000
	Tecnología	Adecuación de controles y procedimientos	2 semanas	0	0
	Subtotal Fase 4				**24000**
Fase 5: Capacitación	Recursos humanos	Facilitadores internos (3 módulos)	6 meses	24000 (salario quincenal de Jefatura RRHH) + 15000 (salario quincenal de Jefatura) + 9000 (salario quincenal del Encargado)	576000
	Tecnología	Plataforma de capacitación / LMS	6 meses	12000 (valor de servicio mensual)	72000
	Evaluaciones	Instrumentos de evaluación por módulo	3 evaluaciones	0	0
	Subtotal Fase 5				**648000**
Fase 6: Evaluación Final	Recursos humanos	Jefatura TI y Gerencia	3 días	15000 (salario quincenal de Jefatura) +	9900

Presupuesto estimado por fase del proyecto					
				9000 (salario quincenal del Encargado)	
	Herramientas	Medición de indicadores y reportes (Realizado en Microsoft Excel y Power BI con licencia)	Licencia	2460 (valor anual)	2460
	Subtotal Fase 6				**12360**
				TOTAL GENERAL DEL PROYECTO	**821244 HNL**

Fuente. Elaboración propia

Tabla 42. Estimación de costos por fase del proyecto

Estimación PERT de costos por fase del proyecto (HNL)					
Fase	**Optimista (O)**	**Más Probable (MP)**	**Pesimista (P)**	**Media Triangular (O + MP + P) /3**	**Distribución Beta (O+4MP+P) /6**
Fase 1: Diagnóstico Inicial	30000	34884	40000	34961.33	34922.66
Fase 2: Diseño del Modelo Integral	60000	66000	70000	65333.33	65666.66
Fase 3: Presentación y Evaluación	30000	36000	40000	35333.33	35666.66

Estimación PERT de costos por fase del proyecto (HNL)					
Fase 4: Implementación del Modelo	20000	24000	32000	25333.33	24666.66
Fase 5: Capacitación	500000	648000	700000	616000	632000
Fase 6: Evaluación Final	10000	12360	15000	12453.33	12406.66
TOTAL DEL PROYECTO	**650000**	**821244**	**897000**		

Fuente. Elaboración propia

Tabla 43. Estimación de tiempos por fase del proyecto

Fase	**Actividad**	**Tiempo MP**	**Tiempo O**	**Tiempo P**	**Duración Estimada (O+4MP+P) /6**	**Varianza σ² (días²)**
Fase 1: Diagnóstico Inicial	Levantamiento de activos	*2 semanas*	*1 semana*	*3 semanas*	*2 semanas*	*2.78*
	Evaluación preliminar de riesgos	*1 semana*	*5 días*	*2 semanas*	*1 semana + 1 día*	*0.69*
Fase 2: Diseño de Modelo Integral	Desarrollo de matriz de evaluación de riesgos basada en ISO 27005	*1 mes*	*2 semanas*	*2 meses*	*1 mes + 2.5 días*	*25*
	Desarrollo de Sistema de Priorización de Vulnerabilidades	*2 meses*	*1 mes*	*2 meses y medio*	*1 mes + 25.5 días*	*25*

Fase	Actividad	Tiempo MP	Tiempo O	Tiempo P	Duración Estimada (O+4MP+P) /6	Varianza σ^2 (días^2)
	Desarrollo de Plan de Capacitación	*1 mes*	*3 semanas*	*1 mes y medio*	*1 mes + 1 día*	*6.25*
Fase 3: Presentación y Evaluación del Modelo	Presentación de Matriz de Evaluación de Riesgos y Sistema de Priorización de Vulnerabilidades	*2 días*	*1 día*	*3 días*	*2 días*	*0.11*
	Presentación del Plan de Capacitación	*1 día*	*1 día*	*2 días*	*1.5 días*	*0.03*
	Ajustes al modelo en base a retroalimentación	*3 semanas*	*2 semana*	*1 mes*	*21 días*	*2.78*
Fase 4: Implementación del Modelo	Implementación de gestión de riesgos y consideración de vulnerabilidades hacia los procesos, activos y operaciones de TI.	*2 semanas*	*1 semana*	*3 semanas*	*2 semanas*	*2.78*
Fase 5: Capacitación	Módulo 1	*2 meses*	*1 mes y medio*	*2 meses y medio*	*2 meses*	*11.11*
	Evaluación del Módulo 1	*2 días*	*1 día*	*3 días*	*2 días*	*0.11*
	Módulo 2	*2 meses*	*1 mes y medio*	*2 meses y medio*	*2 meses*	*11.11*

Fase	Actividad	Tiempo MP	Tiempo O	Tiempo P	Duración Estimada (O+4MP+P) /6	Varianza σ^2 (días^2)
	Evaluación del Módulo 2	*2 días*	*1 día*	*3 días*	*2 días*	*0.11*
	Módulo 3	*2 meses*	*1 mes y medio*	*2 meses y medio*	*2 meses*	*11.11*
	Evaluación del Módulo 3	*2 días*	*1 día*	*3 días*	*2 días*	*0.11*
Fase 6: Evaluación	Evaluación de indicadores de desempeño	*3 días*	*1 día*	*4 días*	*3 días*	*0.25*

Fuente. Elaboración propia

Ruta crítica estimada:

Tomando en cuenta que, para cada fase, excepto la fase 5, que se compone solamente de tareas consecutivas, se debe considerar solamente la actividad que tome más tiempo, ya que se hacen en paralelo.

Duración Total = Fase1 + Fase2 + Fase3 + Fase4 + Fase5 + Fase6

= 10 + 45.5 + 23 + 10 + 126 + 3

= 217.5 días.

Varianza total (sumando todas las varianzas):

- Fase 1: 2.78
- Fase 2: 25
- Fase 3: 0.11
- Fase 4: 2.78
- Fase 5: 11.11 + 0.11 + 11.11 + 0.11 + 11.11 + 0.11
- Fase 6: 0.25

$2.78 + 25 + 0.11 + 2.78 + 2.78 + 11.11 + 0.11 + 11.11 + 0.11 + 11.11 + 0.11 + 0.25 = \mathbf{67.36}$

Cálculo del Intervalo de Confianza al 95%:

Desviación estándar total:

$\sigma = 67.36 \approx 8.207$ días

Margen de error (95% confianza, Z=1.96):

$1.96 * 8.207 \approx 16.08$ días ≈ 3.2 semanas

Duración total estimada:

217.5 días ≈ 10.9 meses

Intervalo de confianza:

10.9 meses ± 3.2 semanas

El proyecto tiene una duración estimada de aproximadamente 10.9 meses, con un intervalo de confianza del 95% de ± 3.2 semanas.

Respecto al Retorno de la Inversión (ROI), se realizaron cálculos importantes, descritos a continuación, para determinar el porcentaje de lo gastado actualmente en sueldos para una jornada habitual de 8 horas y de ese total lo que realmente corresponde para las horas efectivas de trabajo por departamento.

Tratamiento de datos:

1) Del dataset principal correspondiente a los tickets en estado "completado" entre septiembre 2024 y septiembre 2025, se calculó un promedio de tiempo de atención de tickets por departamento, resultando los siguientes tiempos, ver tabla 43

Tabla 44. Promedio de tiempo de atención de tickets por departamento

Departamento	Promedio Tiempo Resolución (hrs)
COMEX	1103.2
Comercial	526.37
Gestión Humana	491.61
Logística	457.44
Créditos y Cobros	423.12

Departamento	Promedio Tiempo Resolución (hrs)
Administración y Finanzas	359.91
Regencia y Calidad	213.49
Contabilidad	207.7
Mejora Continua	193.25
Tecnología Informática	168.46
Marketing	159.89

Fuente. Elaboración propia

2) Trabajando los siguientes resultados en base a los siguientes datos:

- Jornada laboral diaria: 8 horas
- Días laborales semanales: 5 días
- Semanas en el año: 52
- Días laborales en el año: Días laborales semanales * Semanas en el año: 5*52: 260 días

Calculamos:

- Las Horas diarias empleadas por TI en la resolución de tickets por departamento con la siguiente fórmula

  Promedio Tiempo Resolución (horas) / 260 días

  Tomando este resultado como las **horas inactivas de trabajo por departamento**

- Teniendo las horas inactivas de trabajo por departamento, en fácil calcular las **horas efectivas de trabajo por departamento**, ver tabla 44 con resultados.

  8hrs - Horas inactivas de trabajo por departamento

Tabla 45. Horas diarias empleadas por TI en la resolución de tickets por departamento y horas inactivas y efectivas de trabajo por departamento

Departamento que genera tickets	Tiempo promedio de resolución (hrs)	Horas inactivas de trabajo por departamento	Horas efectivas de trabajo por departamento
COMEX	1103.2	4.24	3.76
Comercial	526.37	2.02	5.98
Gestión Humana	491.61	1.89	6.11
Logística	457.44	1.76	6.24
Créditos y Cobros	423.12	1.63	6.37
Administración y Finanzas	359.91	1.38	6.62
Regencia y Calidad	213.49	0.82	7.18
Contabilidad	207.7	0.8	7.2
Mejora Continua	193.25	0.74	7.26
Tecnología Informática	168.46	0.65	7.35
Marketing	159.89	0.61	7.39

Fuente. Elaboración propia

3) En base a lo anterior, se realizan los últimos cálculos, ver tabla 45.

   Importante aclarar el tratamiento previo de datos, del total de los tickets, se eliminaron los duplicados en base al nombre de empleado, para evitar que ese dato salarial se repitiese por departamento para el mismo empleado más de una vez.

   **** Salario: COLUMNA OCULTA POR TEMAS DE CONFIDENCIALIDAD**

   - Salario Diario: Salario / 30
   - Salario por hora: Salario diario / 8
   - Horas inactivas y efectivas de trabajo por departamento se calcularon en el paso 2
   - Salario diario (tiempo efectivo): Horas efectivas de trabajo * Salario por hora

- Salario (tiempo efectivo): Salario diario (tiempo efectivo) * 30

Tabla 46. Tabla resumen de datos salariales Jornada Completa vs Jornada Efectiva

Departamento	Salario diario	Salario por hora	Horas inactivas de trabajo por departamento	Horas efectivas de trabajo por departamento	Salario diario (tiempo efectivo)	Salario (tiempo efectivo)
Administración y Finanzas	3333.333333	416.666667	1.38	6.62	2758.333333	82750
Administración y Finanzas	2000	250	1.38	6.62	1655	49650
Comercial	900	112.5	2.02	5.98	672.75	20182.5
Comercial	1166.666667	145.833333	2.02	5.98	872.083333	26162.5
Comercial	533.333333	66.666667	2.02	5.98	398.666667	11960
Comercial	600	75	2.02	5.98	448.5	13455
Comercial	533.333333	66.666667	2.02	5.98	398.666667	11960
Comercial	700	87.5	2.02	5.98	523.25	15697.5
Comercial	1633.333333	204.166667	2.02	5.98	1220.916667	36627.5
COMEX	600	75	4.24	3.76	282	8460
COMEX	866.666667	108.333333	4.24	3.76	407.333333	12220
Contabilidad	666.666667	83.333333	0	8	666.666667	20000
Contabilidad	633.333333	79.166667	0.8	7.2	570	17100
Contabilidad	633.333333	79.166667	0.8	7.2	570	17100
Contabilidad	733.333333	91.666667	0.8	7.2	660	19800
Contabilidad	633.333333	79.166667	0.8	7.2	570	17100
Contabilidad	1066.666667	133.333333	0.8	7.2	960	28800
Créditos y Cobros	500	62.5	1.63	6.37	398.125	11943.75
Créditos y Cobros	766.666667	95.833333	1.63	6.37	610.458333	18313.75
Créditos y Cobros	566.666667	70.833333	1.63	6.37	451.208333	13536.25
Créditos y Cobros	500	62.5	1.63	6.37	398.125	11943.75
Créditos y Cobros	1133.333333	141.666667	1.63	6.37	902.416667	27072.5

Departamento	Salario diario	Salario por hora	Horas inactivas de trabajo por departamento	Horas efectivas de trabajo por departamento	Salario diario (tiempo efectivo)	Salario (tiempo efectivo)
Gestión Humana	500	62.5	1.89	6.11	381.875	11456.25
Gestión Humana	500	62.5	1.89	6.11	381.875	11456.25
Gestión Humana	666.6666667	83.33333333	1.89	6.11	509.1666667	15275
Gestión Humana	1600	200	1.89	6.11	1222	36660
Logística	600	75	1.76	6.24	468	14040
Logística	600	75	1.76	6.24	468	14040
Logística	766.6666667	95.83333333	1.76	6.24	598	17940
Logística	600	75	1.76	6.24	468	14040
Logística	833.3333333	104.1666667	1.76	6.24	650	19500
Logística	600	75	1.76	6.24	468	14040
Logística	1500	187.5	1.76	6.24	1170	35100
Marketing	1800	225	0.61	7.39	1662.75	49882.5
Marketing	1333.333333	166.6666667	0.61	7.39	1231.666667	36950
Mejora Continua	1333.333333	166.6666667	0.74	7.26	1210	36300
Regencia y Calidad	1533.333333	191.6666667	0.82	7.18	1376.166667	41285
Regencia y Calidad	600	75	0.82	7.18	538.5	16155
Tecnología Informática	1666.666667	208.3333333	0.65	7.35	1531.25	45937.5
Tecnología Informática	600	75	0.65	7.35	551.25	16537.5

Fuente. Elaboración Propia

4) De lo anterior se concluye que

Total de Salarios (mensual) = L 1,150,000.00 (esto solo en base al salario de los empleados que subieron ticket entre el periodo septiembre 2024 y septiembre 2025)

Total de Salarios (mensual, para el tiempo efectivo de trabajo) = L 938,430.00

Total pérdida mensual = Total de Salarios (mensual) - Total de Salarios (mensual, para el tiempo efectivo de trabajo) = 1,150,000 – 938,430 = L 211, 570.00

Total de la pérdida anual = Total pérdida mensual * 12 = 211,570.00 * 12 =

L 2,538,840.00

5) Finalmente, estos resultados en porcentaje para entender mejor las proporciones

   1,150,000 -> 100% (de lo pagado en un mes)

   938,430 -> X?

   Teniendo como resultado que el pago por horas efectivas de trabajo al mes equivale al 82%

   Infiriendo que, porcentaje de la perdida mensual para la empresa en gasto de planilla mensual es del **18%.**

Con el objetivo de complementar el análisis de costos y demostrar la viabilidad económica de nuestra propuesta presentada, se ha desarrollado el siguiente análisis financiero, orientado a cuantificar los beneficios monetarios derivados de la mejora en la eficiencia operativa del área de TI de Distribuidora Leterago Honduras.

El análisis se fundamenta en dos componentes:

1. El ahorro generado por la reducción del Tiempo Medio de Respuesta (MTTR), y
2. El cálculo del Retorno de la Inversión (ROI).

Para efectos del análisis, se establecen los siguientes supuestos financieros, basados en la información recopilada durante el desarrollo de la investigación:

- Costo total del proyecto (Ver tabla 40): L 821,244
- MTTR actual promedio: 391.31 horas (promedio de los tiempos de resolución de los 247 casos presentados durante un año)
- MTTR esperado posterior a la implementación: 391.31 * 0.5 = 195.66 (se espera una reducción de al menos un 50% en el MTTR actual)
- Salario mensual promedio del personal de TI: L 24,000
- Incidentes promedio atendidos por año: 247 casos
- Jornada laboral mensual estimada: 160 horas

A partir de estos valores, se estima el costo promedio por hora del personal de TI:

Costo por hora = 24,000/160 = 150 Lempiras/hora

1. Ahorro operativo por reducción del Tiempo Medio de Respuesta (MTTR)

La reducción de tiempo por incidente se calcula como:

Reducción de MTTR = 391.31 – 195.66 = 195.65 horas

El ahorro económico por incidente es:

195.65*150 = 29,347.5 Lempiras

Considerando un promedio de 247 incidentes anuales, el ahorro económico anual estimado es:

29,347.5* 247 = 7,248,832.5 Lempiras

Este monto representa el ahorro directo anual derivado exclusivamente de la reducción del tiempo de respuesta del área de TI.

2. Cálculo del Retorno de la Inversión (ROI)

Para evaluar el retorno de la inversión, se aplica el indicador de Retorno de la Inversión (ROI), conforme a la siguiente fórmula:

ROI = (Beneficio - Costo de la inversión) / Costo de la inversión

Sustituyendo los valores obtenidos:

ROI= (7,248,832.5 - 821,244) / 821,244

ROI= 7.83

Esto indica que, por cada lempira invertido en la implementación del proyecto, la organización obtiene un retorno aproximado de L 7.83, lo cual evidencia una relación beneficio–costo bastante favorable.

6.7 GESTIÓN DEL CAMBIO

Visión y Comunicación: Comunicar el "por qué" y los beneficios esperados con la implementación del proyecto desde la alta dirección hacia toda la organización. Canales: correos, reuniones, social media interna.

Patrocinio y Roles: Se designará un Sponsor Ejecutivo (Gerente General Leterago

CEAM) y un Propietario del Cambio (Gerente de TI CEAM). Se formará un Grupo Guía con representantes de áreas clave (Finanzas, Logística, Comercial).

Capacitación y Soporte:

- Equipo TI Honduras: Asistencia, capacitación y soporte local.
- Líderes y demás personal administrativo: Talleres sobre políticas nuevas y su rol en el despliegue y adopción del proyecto.

Aprendizaje continuo: Plataforma web (Moodle).

Métricas de Adopción: Se medirá no solo el avance técnico, sino también el porcentaje de personal capacitado, resultados de encuestas de percepción de adopción del proyecto, y reducción en incidentes por error humano.

Riesgos de Implementación y Mitigación:

- Riesgo: Falta de compromiso de la alta dirección. Mitigación: Presentar propuesta con ROI estimado vinculado a reducción de MTTR y los beneficios de formación en riesgos de seguridad de la información.
- Riesgo: Sobrecarga del personal de TI. Mitigación: Implementación por fases, priorización con la nueva matriz de criticidad, y considerar consultoría externa inicial.
- Riesgo: Rechazo cultural a la formalización. Mitigación: Involucrar a usuarios desde el diseño de flujos.

Tabla 47. Presupuesto OPEX/CAPEX

Item	Descripción	Tipo (CAPEX/OPEX)	Costo Unitario (USD)	Costo Total (USD)	Justificación
OPEX (Gastos Operativos Recurrentes)					

Item	Descripción	Tipo (CAPEX/OPEX)	Costo Unitario (USD)	Costo Total (USD)	Justificación
1	Licencias software gestión de riesgos	OPEX	7,692	15,384	Herramienta central para el marco.
2	Medición de indicadores y reportes (Realizado en Microsoft Excel y Power BI con licencia)		2,460	2,460	Herramienta central para el marco.
3	Licencia Moodle		12,000	72,000	Herramienta central para el marco.
4	Consultoría interna (6 meses)		24,000/mes	576,000	24000 (salario quincenal de Jefatura RRHH) + 15000 (salario quincenal de Jefatura) + 9000 (salario quincenal del Encargado
5	Evaluación		9900	9,900	15000 (salario quincenal de Jefatura) + 9000 (salario quincenal del Encargado)
6	Implementación		24000	24,000	15000 (salario quincenal de Jefatura) + 9000 (salario

Item	Descripción	Tipo (CAPEX/OPEX)	Costo Unitario (USD)	Costo Total (USD)	Justificación
					quincenal del Encargado)
7	Presentación		15000	36,000	15000 (salario quincenal de Jefatura) + 9000 (salario quincenal del Encargado)
8	Encargado TI (Calculo de CVSS 4.0)	9000	36,000	9000 (salario quincenal)	
9	Jefatura TI (matriz ISO 27005)	15000	30,000	15000 (salario quincenal)	
10	Encargado TI (evaluación preliminar de riesgos)	4500	4,500	4500 (salario semanal)	
11	Evaluación Inicial		15000	15,000	15000 (salario quincenal)
	TOTAL CAPEX			**0**	
	TOTAL OPEX (Año 1)			**821244**	
	INVERSIÓN TOTAL AÑO 1			**821244**	

Fuente. Elaboración propia

El 100% de los costos identificados corresponden a OPEX, ya que:

No se adquieren activos tecnológicos propios.

No se desarrolla software a medida capitalizable.

Todos los costos están asociados a:

- Licencias
- Salarios
- Consultoría interna
- Actividades de análisis e implementación

6.8 CONCORDANCIA DE LOS SEGMENTOS DE LA TESIS CON LA PROPUESTA

La siguiente tabla tiene como propósito sintetizar el trayecto de toda la investigación para poder mostrar la relación transversal que existe entre el fenómeno que se propuso investigar, lo encontrado y lo que se propone para abordar los puntos de mejora identificados.

Tabla 48. Tabla de resumen de concordancia Tesis y Propuesta

Capítulo 1			**Capítulo 2**	**Capítulo 3**			**Capítulo 5**	**Capítulo 6**	
Título de Investigación	Objetivo General	Objetivos Específicos	Teorías de Sustento	Variables	Poblaciones	Técnicas	Conclusiones	Nombre de Propuesta	Objetivos de Propuesta
BRECHA DE CONOCIMIENTO EN LA GESTIÓN DE RIESGOS DE TI PARA EL ÁREA ADMINISTRATIVA EN EL SECTOR FARMACÉUTICO HONDUREÑO: ESTUDIO DE CASO EN DISTRIBUIDORA LETERA	Diagnosticar la brecha de conocimiento en la gestión de riesgos dentro del área de TI de Distribuidora Leterago para determinar su impacto en la exposición a vulnera	Determinar el nivel de conocimiento sobre gestión de riesgos en el personal de TI, (M) utilizando una matriz de competencias basada en ISO 27005 y (A) encuestas a	Teoría del Agente - Principal	Brecha de Conocimiento	Totalidad de empleados activos que pertenecen a Distribuidora Leterago y Laboratorios Megalabs **132 empleados activos**	Muestreo por cuotas		**MODELO INTEGRAL DE GESTIÓN DE RIESGOS PARA EL ÁREA DE TI BASADO EN NORMATIVA ISO 27005 Y**	**Objetivo 1** Diseñare implementar, dentro de un periodo máximo de 12 meses, un modelo integral de gestión de riesgos para el área de TI, que incorpore instrum

Capítulo 1			Capítulo 2		Capítulo 3		Capítulo 5	Capítulo 6	
GO Y LABORATORIO MEGALABS 2025	bilidades y la eficiencia operativa, (M) mediante encuestas y análisis documental de reportes de incidentes, (R) para generar un diagnóstico base que informe futuras estrategias de mitigación, (T) durante el último trimestre de 2025.	todo el personal del área, (R) para cuantificar la brecha de habilidades, (T) en un plazo de cinco semanas.			Muestra de **41 personas.**			**CVSS 4.0 PARA DISTRIBUIDORA LETERAGO EN HONDURAS.**	entos de medición y monitoreo, utilizando normativas como ISO 27005, con el fin de fortalecer el nivel de gobernanza institucional y asegurando su cumplimiento mediante la aplicación de indicadores de desempeño definidos previamente.

Capítulo 1		Capítulo 2		Capítulo 3			Capítulo 5	Capítulo 6	
		Identificar los factores organizacionales que perpetúan la brecha de conocimiento, (M) mediante el análisis de la documentación de políticas y (A) encuestas con los líderes de equipo, (R) para comprender las causas raíz culturales, (T) en un plazo de seis semanas.	Teoría del Aprendizaje Organizacional	Factores Organizacionales					**Objetivo 2** Documentar la clasificación de los activos de TI, la elaboración de una matriz de riesgos de TI y la priorización de vulnerabilidades con el propósito de disminuir el MTTR dentro de un periodo máximo de 9 meses.

Capítulo 1		Capítulo 2		Capítulo 3			Capítulo 5	Capítulo 6	
		Determinar el nivel de eficiencia operativa por medio de la respuesta a incidentes, (M) analizando el Tiempo Medio de Respuesta (MTTR) de los (A) incidentes reportados en los últimos 12 meses, (R) para conectar la brecha de conocimiento con resultados operativ		Eficiencia Operativa					**Objetivo 3** Diseñar e implementar, durante un periodo máximo de 9 meses, un plan de capacitación dirigido al personal administrativo de la filial en Honduras de Distribuidora Lteragro, logrando una cobertura mínima del 80 % del personal involucrado,

Capítulo 1			Capítulo 2	Capítulo 3		Capítulo 5	Capítulo 6	
		os, (T) en un plazo de ocho semanas.						con el propósito de disminuir la dependencia actual hacia el área de TI para las operaciones diarias y orientando a un cambio positivo de la cultura organizacional.

Fuente. Elaboración propia

REFERENCIAS BIBLIOGRÁFICAS

Aguilar Gavira, S., & Barroso Osuna, J. (2015). La triangulación de datos como estrategia en investigación educativa. *Píxel-Bit, Revista de Medios y Educación*, (47), 73–88. https://doi.org/10.12795/pixelbit.2015.i47.05

AL-Dosari, K., & Fetais, N. (2023). Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach. *Electronics*, *12*(17), 3629. https://doi.org/10.3390/electronics12173629

Arias, F. G. (2012). *El Proyecto de Investigación: Introducción a la metodología científica* (Sixth). Editorial Episteme. https://abacoenred.org/wp-content/uploads/2019/02/El-proyecto-de-investigaci%C3%B3n-F.G.-Arias-2012-pdf-1.pdf

Arias González, J. L., & Covinos Gallardo, M. (2021). *Diseño y Metodología de la Investigación* (First). Enfoques Consulting EIRL. https://www.academia.edu/69037546/Arias_Covinos_Dise%C3%B1o_y_metodologia_de_la_investigacion_1_

ASAMBLEA LEGISLATIVA DE LA REPUBLICA DE EL SALVADOR. (2024, noviembre 15). *Ley de Ciberseguridad y Seguridad de la Información – Decreto No. 143*. DIARIO OFICIAL. https://www.diariooficial.gob.sv/seleccion/31396

Beltrán Hernández, C. R., Ramirez, L. V. C., Martínez, C. A. S., & Diaz, J. L. (2023). *EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN EN TRUESECURE S.A. UTILIZANDO LA METODOLOGÍA MAGERIT Y PLAN DE TRATAMIENTO DE RIESGOS.* https://repositorio.unbosque.edu.co/server/api/core/bitstreams/75131c2d-5d90-40e0-a81d-b066bac6c5e2/content

Brandon-Jones, A., & Slack, N. (Eds.). (2019). *Operations Management* (9. Auflage). Pearson Education, Limited.

Castro Mecias, L. T. (2014). *Guía de gestión del riesgo tecnológico para el tratamiento de la seguridad durante el proceso de desarrollo de software.* [Universidad de las Ciencias Informáticas]. https://repositorio.uci.cu/bitstream/ident/8654/1/Lilian%20Teresa%20Castro%20Mecias-TM.pdf

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology* (NIST SP 800-61r2; p. NIST SP 800-61r2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

Colman, A. M. (2009). *A dictionary of psychology* (Third ed). Oxford university press.

Comisión Nacional de Bancos y Seguros (CNBS). (2022, diciembre 19). *NORMAS PARA LA GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN, CIBERSEGURIDAD Y CONTINUIDAD DEL NEGOCIO*. https://circulares.cnbs.gob.hn/Archivo/Viewer/2520/025-2022%20NORMAS%20GESTION%20TECNOLOGIAS%20INFORMACION.pdf

CONGRESO DE LA REPÚBLICA DE PERÚ. (2011, julio 3). *LEY N°29733: LEY DE PROTECCIÓN DE DATOS PERSONALES*. PODER LEGISLATIVO DE PERÚ. https://www.leyes.congreso.gob.pe/documentos/leyes/29733.pdf

Dávila Angeles, A. A., & Dextre Alarcón, B. J. (2021). *Propuesta de una Implementación de un programa de Gestión de Vulnerabilidades de Seguridad Informática para mitigar los siniestros de la información en el policlínico de salud AMC alineado a la NTP-ISO/IEC 27001:2014 en la ciudad de Lima—2021* [Universidad Tecnológica del Perú]. https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/4906/A.Davila_B.Dextre_Tesis_Titulo_Profesional_2021.pdf;jsessionid=90431CC361C46934A802EDB61DE239FF?sequence=1

Denzin, N. K. (1978). *Sociological methods: A sourcebook* (2d ed). McGraw-Hill.

Dirección Nacional de Gobernanza de TI. (2017, agosto 29). *Normas Generales para la Gestión de las*

Tecnologías de la Información y Comunicación en el Estado. AUTORIDAD NACIONAL PARA LA INNOVACIÓN GUBERNAMENTAL. https://aig.gob.pa/descargas/2019/06/normas-generales-para-la-gestion-de-las-tic-en-el-estado-version-1.pdf

e-Governance Academy. (2024, septiembre 9). *About us » E-riigi Akadeemia*. E-Governance Academy. https://ega.ee/about-us/

e-Governance Academy Foundation. (2023a, agosto 1). *National Cyber Security Index 3.0 Methodology*. NCSI. https://ega.ee/wp-content/uploads/2023/08/NCSI-3.0_Methodology.pdf

e-Governance Academy Foundation. (2023b, septiembre 1). *National Cyber Security Index—Ranking*. National Cyber Security Index. https://ncsi.ega.ee/ncsi-index/?archive=1

Eisenhardt, K. M. (1989). Agency Theory: An Assessment and Review. *The Academy of Management Review*, *14*(1), 57–74. https://doi.org/10.2307/258191

European Commission. (2004, marzo). *Project Cycle Management Guidelines*. EuropeAid Cooperation Office. https://www.iwlearn.net/resolveuid/6044b286-0674-40db-9043-a947532161cd

European Confederation of Institutes of Internal Auditing. (2021, septiembre 1). *RISK IN FOCUS 2022: Hot topics for internal auditors*. European Confederation of Institutes of Internal Auditing. https://www.eciia.eu/wp-content/uploads/2021/09/FINAL-Risk-in-Focus-2022-V11.pdf

Fiol, C. M., & Lyles, M. A. (1985). Organizational Learning. *The Academy of Management Review*, *10*(4), 803–813. https://doi.org/10.2307/258048

He, Y., & Johnson, C. (2017). Challenges of information security incident learning: An industrial case study in a Chinese healthcare organization. *Informatics for Health and Social Care*, *42*(4), 393–408.

Hernández Sampieri, R., Fernandez-Collado, C. F., & Lucio Baptista, M. del P. (2014). *Metodología de la investigación* (P. Baptista Lucio, Ed.; Sexta edición). McGraw-Hill Education.

Hernández Sampieri, R., & Mendoza Torres, C. P. (2018). *Metodología de la investigación: Las rutas*

cuantitativa, cualitativa y mixta (First edition). McGraw-Hill Education.

IBM. (2025). *Informe "Cost of a Data Breach" de 2025: La brecha en la supervisión de la IA* (Cost of a Data Breach, p. 8). IBM.

INCIBE. (2015). *Gestión de riesgos: Una guía de aproximación para el empresario.* https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf

International Organization for Standardization (ISO). (2018). *ISO/IEC 27000:2018(en), Information technology—Security techniques—Information security management systems—Overview and vocabulary*. ISO. Online Browsing Platform (OBP). https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27000:ed-5:v1:en

International Organization for Standardization (ISO). (2022). *ISO/IEC 27005:2022(en), Information security, cybersecurity, and privacy protection—Guidance on managing information security risks*. ISO. Online Browsing Platform (OBP). https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27005:ed-4:v1:en

International Telecommunication Union (ITU). (2024, junio 1). *Global Cybersecurity Index 2024*. International Telecommunication Union (ITU). https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

ISACA. (2012). *COBIT® 2019 Framework: Introduction and methodology*. ISACA.

JUNTA MONETARIA, BANCO DE GUATEMALA. (2021, enero 12). *Reglamento para la Administración del Riesgo Tecnológico—ANEXO A LA RESOLUCIÓN JM-104-2021*. DIARIO DE CENTROAMÉRICA. https://banguat.gob.gt/sites/default/files/banguat/Publica/Res_JM/2021/Res_JM-104-2021.pdf

Knime. (s/f-a). Crosstab [Hub]. *Knime Community Hub*. Recuperado https://hub.knime.com/knime/extensions/org.knime.features.base/latest/org.knime.base.node.viz.crosstable.CrosstabNodeFactory

Knime. (s/f-b). Decision Tree Predictor [Hub]. *Knime Community Hub*. Recuperado https://hub.knime.com/knime/extensions/org.knime.features.base/latest/org.knime.base.node.mine.decisiontree2.predictor2.DecTreePredictorNodeFactory

Knime. (s/f-c). Numeric Binner [Hub]. *Knime Community Hub*. Recuperado https://hub.knime.com/knime/extensions/org.knime.features.base/latest/org.knime.base.node.preproc.binner.BinnerNodeFactory

Knime. (s/f-d). Numeric Scorer [Hub]. *Knime Community Hub*. Recuperado https://hub.knime.com/knime/extensions/org.knime.features.base/latest/org.knime.base.node.mine.scorer.numeric2.NumericScorer2NodeFactory

Knime. (s/f-e). Polynomial Regression Learner [Hub]. *Knime Community Hub*. Recuperado https://hub.knime.com/knime/extensions/org.knime.features.base/latest/org.knime.base.node.mine.regression.polynomial.learner2.PolyRegLearnerNodeFactory2

Knime. (s/f-f). Regression Predictor [Hub]. *Knime Community Hub*. Recuperado https://hub.knime.com/knime/extensions/org.knime.features.base/latest/org.knime.base.node.mine.regression.predict3.RegressionPredictorNodeFactory2

Knime. (s/f-g). Scorer (JavaScript) [Hub]. *Knime Community Hub*. Recuperado https://hub.knime.com/knime/extensions/org.knime.features.js.views.labs/latest/org.knime.js.base.node.scorer.ScorerNodeFactory

McCarthy, J., Mamula, D., Brule, J., Meldorf, K., Jennings, R., Wiltberger, J., Thorpe, C., Dombrowski, J., Lattin, O., & Sepassi, S. (2023). *Cybersecurity framework profile for hybrid satellite networks (HSN)* (NIST IR 8441; p. NIST IR 8441). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.IR.8441

Nakash, M., & Bouhnik, D. (2020). Risks in the absence of optimal knowledge management in knowledge-intensive organizations. *VINE Journal of Information and Knowledge Management*

Systems, *52*(1), 1–157. https://doi.org/10.1108/VJIKMS-05-2020-0081

Narro Mestanza, S. M. (2021). *EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y LA GESTIÓN DE RIESGOS EN EL ÁREA INFORMÁTICA DE UNA UNIVERSIDAD PÚBLICA, REGIÓN CAJAMARCA 2020* [Universidad Privada del Norte]. https://repositorio.upn.edu.pe/bitstream/handle/11537/30041/Narro%20Mestanza%20Sarita%20Morelia.pdf?sequence=1&isAllowed=y

NIST. (2011, marzo 1). *NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View*. NIST. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

NIST. (2024). *Spanish Translation of the NIST Cybersecurity Framework 2.0* (NIST CSWP 29 spa; p. NIST CSWP 29 spa). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29.spa

O'Sullivan, A., & Sheffrin, S. M. (2004). *Economics: Principles in action*. Recording for the Blind & Dyslexic.

Pandey, S., Rathod, B. R., & Kothari, A. (2022). *The Inclusive Internet Index 2022: Executive summary* (p. 21). Economist Impact. https://impact.economist.com/projects/inclusive-internet-index/downloads/ei-meta_3i_5yr_lookback_report_0.pdf

Pirani. (2022, diciembre 1). *Estudio de Gestión de Riesgos 2022*. Pirani. https://www.piranirisk.com/es/academia/especiales/estudio-de-gestion-de-riesgos-en-latinoamerica-2022

Putra, A. P., & Soewito, B. (2023). Integrated Methodology for Information Security Risk Management using ISO 27005:2018 and NIST SP 800-30 for Insurance Sector. *International Journal of Advanced Computer Science and Applications*, *14*(4), 975.

Ramos Galarza, C. A. (2020). Los alcances de una investigación. *CienciAmérica: Revista de divulgación*

científica de la Universidad Tecnológica Indoamérica, *9*(3), 1–6.

REPUBLIC OF KENYA. (2019, noviembre 25). *THE DATA PROTECTION ACT*. REPUBLIC OF KENYA. https://www.kentrade.go.ke/wp-content/uploads/2022/09/Data-Protection-Act-1.pdf

REPUBLIC OF SINGAPORE. (2018, marzo 12). *CYBERSECURITY ACT 2018*. GOVERNMENT GAZETTE. https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312?DocDate=20180312&ViewType=Pdf&_=20250321180130

SIECA. (2025a, mayo). *Monitor del comercio de bienes. Cuarto trimestre de 2024*. https://estadisticas.sieca.int/documentos/detalle/4273

SIECA. (2025b, agosto 26). *Sistemas de Estadísticas y Análisis de Mercado de Comercio de Centro América*. https://www.sec.sieca.int/

Siegel, S. (1995). *Estadística no paramétrica aplicada a las ciencias de la conducta* (1a. ed). Trillas.

Solís García, S., Montillano Vivas, M., Chinchilla Sáenz, S., Tenorio Chacón, O., Badilla Picado, I., & Lemaitre Picado, R. (2021, octubre 11). *Normas técnicas para la gestión y el control de las Tecnologías de Información*. Ministerio de Cultura y Juventud de Costa Rica. https://www.mcj.go.cr/sites/default/files/2021-12/MICITT~2.PDF

SUPERINTENDENCIA DE BANCOS Y DE OTRAS INSTITUCIONES FINANCIERAS. (2007, octubre 30). *NORMA SOBRE GESTIÓN DE RIESGO TECNOLÓGICO Resolución N^{o} CD-SIBOIF-500-1-SEP19-2007*. LA GACETA. http://legislacion.asamblea.gob.ni/gacetas/2007/10/g208.pdf

Tassey, G. (1992). *Technology Infrastructure and Competitive Position*. Springer US. https://doi.org/10.1007/978-1-4615-3608-6

Anexo 2: POBLACIÓN DE ESTUDIO.

ID	Área o Puesto	Empresa Perteneciente	Tipo de Empleado
1	ADMINISTRACIÓN Y FINANZAS	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
2	ADMINISTRACIÓN Y FINANZAS	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
3	ADMINISTRACIÓN Y FINANZAS	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
4	ADMINISTRACIÓN Y FINANZAS	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
5	ADMINISTRACIÓN Y FINANZAS	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
6	ADMINISTRACIÓN Y FINANZAS	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
7	ADMINISTRACIÓN Y FINANZAS	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
8	ADMINISTRACIÓN Y FINANZAS	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
9	ADMINISTRACIÓN Y FINANZAS	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
10	ADMINISTRACIÓN Y FINANZAS	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
11	ADMINISTRACIÓN Y FINANZAS	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
12	ADMINISTRACIÓN Y FINANZAS	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
13	ADMINISTRACIÓN Y FINANZAS	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
14	COMERCIAL	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
15	COMERCIAL	DISTRIBUIDORA LETERAGO	OPERATIVO
16	COMERCIAL	DISTRIBUIDORA LETERAGO	OPERATIVO
17	COMERCIAL	DISTRIBUIDORA LETERAGO	OPERATIVO
18	COMERCIAL	DISTRIBUIDORA LETERAGO	OPERATIVO
19	COMERCIAL	DISTRIBUIDORA LETERAGO	OPERATIVO
20	COMERCIAL	DISTRIBUIDORA LETERAGO	OPERATIVO
21	COMERCIAL	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO

22	COMERCIAL	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
23	COMERCIAL	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
24	COMERCIAL	DISTRIBUIDORA LETERAGO	OPERATIVO
25	COMERCIAL	DISTRIBUIDORA LETERAGO	OPERATIVO
26	COMERCIAL	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
27	COMERCIAL	DISTRIBUIDORA LETERAGO	OPERATIVO
28	COMERCIAL	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
29	OPERACIONES	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
30	OPERACIONES	DISTRIBUIDORA LETERAGO	OPERATIVO
31	OPERACIONES	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
32	OPERACIONES	DISTRIBUIDORA LETERAGO	OPERATIVO
33	OPERACIONES	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
34	OPERACIONES	DISTRIBUIDORA LETERAGO	OPERATIVO
35	OPERACIONES	DISTRIBUIDORA LETERAGO	OPERATIVO
36	OPERACIONES	DISTRIBUIDORA LETERAGO	OPERATIVO
37	OPERACIONES	DISTRIBUIDORA LETERAGO	OPERATIVO
38	OPERACIONES	DISTRIBUIDORA LETERAGO	OPERATIVO
39	OPERACIONES	DISTRIBUIDORA LETERAGO	OPERATIVO
40	OPERACIONES	DISTRIBUIDORA LETERAGO	OPERATIVO
41	OPERACIONES	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
42	OPERACIONES	DISTRIBUIDORA LETERAGO	OPERATIVO
43	OPERACIONES	DISTRIBUIDORA LETERAGO	OPERATIVO
44	OPERACIONES	DISTRIBUIDORA LETERAGO	OPERATIVO
45	OPERACIONES	DISTRIBUIDORA LETERAGO	OPERATIVO

46	PERSONAS & CULTURA	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
47	PERSONAS & CULTURA	DISTRIBUIDORA LETERAGO	OPERATIVO
48	PERSONAS & CULTURA	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
49	REGENCIA Y CALIDAD	DISTRIBUIDORA LETERAGO	OPERATIVO
50	REGENCIA Y CALIDAD	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
51	REGENCIA Y CALIDAD	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
52	REGIONAL	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
53	TECNOLOGÍA INFORMÁTICA	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
54	TECNOLOGÍA INFORMÁTICA	DISTRIBUIDORA LETERAGO	ADMINISTRATIVO
55	SUPERVISOR	LABORATORIO MEGALABS	ADMINISTRATIVO
56	SUPERVISOR	LABORATORIO MEGALABS	ADMINISTRATIVO
57	KEY ACCOUNT MANAGER OTC	LABORATORIO MEGALABS	ADMINISTRATIVO
58	SUPERVISOR	LABORATORIO MEGALABS	ADMINISTRATIVO
59	SUPERVISOR	LABORATORIO MEGALABS	ADMINISTRATIVO
60	SUPERVISOR	LABORATORIO MEGALABS	ADMINISTRATIVO
61	KEY ACCOUNT MANAGER	LABORATORIO MEGALABS	ADMINISTRATIVO
62	SUPERVISOR	LABORATORIO MEGALABS	ADMINISTRATIVO
63	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
64	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
65	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
66	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
67	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
68	ASESOR NUTRICIONAL	LABORATORIO MEGALABS	OPERATIVO
69	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO

70	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
71	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
72	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
73	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
74	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
75	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
76	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
77	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
78	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
79	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
80	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
81	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
82	PROMOTOR	LABORATORIO MEGALABS	OPERATIVO
83	PROMOTOR OTC	LABORATORIO MEGALABS	OPERATIVO
84	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
85	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
86	VISITADOR MÉDICO DE LINEA	LABORATORIO MEGALABS	OPERATIVO
87	VISITA MÉDICA FDV II	LABORATORIO MEGALABS	OPERATIVO
88	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
89	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
90	VISITA MÉDICA	LABORATORIO MEGALABS	OPERATIVO
91	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
92	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
93	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO

94	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
95	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
96	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
97	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
98	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
99	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
100	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
101	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
102	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
103	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
104	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
105	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
106	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
107	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
108	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
109	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
110	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
111	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
112	PROMOTOR	LABORATORIO MEGALABS	OPERATIVO
113	PROMOTOR	LABORATORIO MEGALABS	OPERATIVO
114	PROMOTOR	LABORATORIO MEGALABS	OPERATIVO
115	PROMOTOR	LABORATORIO MEGALABS	OPERATIVO
116	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
117	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO

118	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
119	ASESOR NUTRICIONAL	LABORATORIO MEGALABS	OPERATIVO
120	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
121	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
122	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
123	ASESOR NUTRICIONAL	LABORATORIO MEGALABS	OPERATIVO
124	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
125	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
126	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
127	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
128	VISITADOR MÉDICO	LABORATORIO MEGALABS	OPERATIVO
129	ASUNTOS REGULATORIOS	LABORATORIO MEGALABS	ADMINISTRATIVO
130	COMMUNITY MANAGER	LABORATORIO MEGALABS	ADMINISTRATIVO
131	GERENTE DE PRODUCTO	LABORATORIO MEGALABS	ADMINISTRATIVO
132	JEFE DE FORMACIÓN MÉDICA	LABORATORIO MEGALABS	ADMINISTRATIVO

Anexo 3: ENCUESTA ESTRUCTURADA.

Conocimientos sobre Gestión de Riesgos de TI en Distribuidora Leterago y Laboratorios Megalabs

Estimado/a colaborador/a,

Con el propósito de desarrollar la investigación de maestría llamada BRECHA DE CONOCIMIENTO EN LA GESTIÓN DE RIESGOS DE TI EN EL SECTOR FARMACEÚTICO HONDUREÑO: ESTUDIO DE CASO EN DISTRIBUIDORA LETERAGO Y LABORATORIOS MEGALABS 2025, esta encuesta tiene como objetivo evaluar el nivel de conocimiento, las prácticas actuales y las percepciones respecto a la gestión de riesgos en el área de Tecnologías de la Información (TI).

Le agradecemos de antemano su tiempo y honestidad.

Instrucciones:

Para cada pregunta, seleccione la opción que mejor represente su opinión o experiencia.

Sección 1: Datos Generales

Departamento en el que trabaja:

- Administración y Finanzas
- Comercial
- Personas y Cultura
- Regencia y Calidad
- Visitas Médicas
- Gerencia
- Otro: _____

¿Qué tipo de sistemas de TI utiliza regularmente en sus labores diarias? (Seleccione todas las que apliquen)

- ERP (Sistema de Planificación de Recursos Empresariales, como ser Microsoft Dynamics)
- Plataforma de correo electrónico (Outlook, Gmail)
- Herramientas de oficina (Suite de Microsoft Office)
- Otro: _____

¿Cuál de las siguientes opciones describe mejor su rol principal en la organización?

- Liderazgo / Supervisión (tengo personal a mi cargo)
- Colaborador Técnico / Especializado (mi rol requiere conocimientos técnicos específicos)
- Colaborador Administrativo / Soporte (mi rol se centra en tareas administrativas y de soporte)

Sección 2: Conocimiento y Concientización

Siguiendo una escala del 1 al 5, donde 1 representa "Nada Importante" y 5 representa "Muy Importante", califique las siguientes afirmaciones según su criterio personal:

La ciberseguridad y la gestión de riesgos de TI para contribuir a la eficiencia operativa de la empresa.

1 2 3 4 5

La ciberseguridad debe ser para proteger los datos de clientes y proveedores.

1 2 3 4 5

Se debe contar con un plan de recuperación ante desastres orientados al área de TI.

1 2 3 4 5

Capacitar continuamente al personal en riesgos cibernéticos.

1 2 3 4 5

Siguiendo una escala del 1 al 5, donde 1 representa "Nada Urgente" y 5 representa "Muy Urgente", califique las siguientes situaciones según su criterio personal:

Un ataque de ransomware que bloquee el acceso a los sistemas de pedidos e inventario.

1 2 3 4 5

Una filtración de datos confidenciales de clientes o productos.

1 2 3 4 5

La caída prolongada del sistema ERP, impidiendo facturar o gestionar envíos.

1 2 3 4 5

El error humano interno (ej.: enviar un correo importante a la persona equivocada).

1 2 3 4 5

El incumplimiento de regulaciones farmacéuticas (ej.: trazabilidad de medicamentos).

1 2 3 4 5

Sección 3: Evaluación de Competencias

La siguiente sección tiene como propósito medir conocimientos sobre la gestión de TI a nivel técnico, por lo que si desconoce la respuesta escriba "Sin respuesta".

Liste 3 activos tecnológicos clave de la empresa y describa los riesgos asociados a la confidencialidad, integridad y disponibilidad.

¿Qué proceso seguiría en caso de detectar un virus dentro de los sistemas de la empresa (considere el ERP, el almacenamiento en la nube o las carpetas compartidas)? Detalle paso a paso su forma de evaluar el riesgo y las acciones que tomaría.

En el caso hipotético de que un ex-compañero de trabajo filtre información sensible de la empresa, proponga 3 controles para tratar esta situación. (Tome en cuenta 3 tipos de tratamiento: Preventivo, Detectivo y Correctivo)

Sección 4: Experiencias y Prácticas

¿Ha recibido formación sobre cómo detectar amenazas de ciberseguridad como phishing o malware?

- Sí, de forma regular y actualizada.
- Sí, pero hace mucho tiempo
- No, nunca.
- No estoy seguro/a.

En el último año, ¿ha experimentado o presenciado algún incidente relacionado con la seguridad de la información? (ej.: correo phishing, ransomware, caída de sistemas críticos, pérdida de datos)

- Sí, en múltiples ocasiones.
- Sí, en una ocasión.
- No, nunca.
- Prefiero no responder.

Si respondió "Sí" a la pregunta anterior, ¿cómo manejó o reportó el incidente?

- Reporté inmediatamente al departamento de TI.
- Lo reporté a mi supervisor/a
- Intenté resolverlo por mi cuenta.
- No supe qué hacer / No lo reporté.
- No aplica.

¿Con qué frecuencia realiza copias de seguridad (backups) de la información crítica de su trabajo hacia su directorio de nube asignado?

- Diariamente
- Semanalmente
- Mensualmente
- Solo cuando me lo indican
- Nunca / No sé cómo hacerlo

Sección 4: Comentarios y Sugerencias

Desde su perspectiva, ¿cuál es el mayor riesgo de TI al que se enfrenta nuestra empresa?

¿Qué tipo de apoyo, recursos o capacitación cree que necesita para contribuir mejor a la seguridad de la información de la empresa?

¡Gracias por su participación!

Su retroalimentación es invaluable para ayudarnos a desarrollar nuestra investigación dentro del área.

Anexo 4: ENLACE A ENCUESTA ESTRUCTURADA Y VISUALIZACIÓN DEL INSTRUMENTO CREADO.

https://forms.cloud.microsoft/Pages/DesignPageV2.aspx?subpage=design&FormId=DQSIkWdsW0yxEjajBLZtrQAAAAAAAAAAAAYAAKBVJ_FURENOQVg3SldCMUFaQlFMSEZCSzlLS082RS4u&Token=6b7090e4d644426e9bd4169a7eda6fb6

Conocimientos sobre Gestion de Riesgos en TI: Distribuidora Leterago/Laboratorios Megalabs

Estimado/a colaborador/a,
Con el propósito de desarrollar la investigación de maestría llamada **BRECHA DE CONOCIMIENTO EN LA GESTIÓN DE RIESGOS DE TI PARA EL ÁREA ADMINISTRATIVA EN EL SECTOR FARMACÉUTICO HONDUREÑO: ESTUDIO DE CASO EN DISTRIBUIDORA LETERAGO Y LABORATORIO MEGALABS 2025**, esta encuesta tiene como objetivo evaluar el nivel de conocimiento, las prácticas actuales y las percepciones respecto a la gestión de riesgos en el área de Tecnologías de la Información (TI). Sus respuestas nos ayudarán a comprender las experiencias, prácticas y necesidades en torno a la seguridad de la información dentro de la empresa. Le agradecemos de antemano su tiempo y honestidad.

Cuando envíe este formulario, no recopilará automáticamente sus detalles, como el nombre y la dirección de correo electrónico, a menos que lo proporcione usted mismo.

* Obligatorio

Seccion 1: Datos Generales

1. ¿En qué departamento trabaja? *

- ◯ Administración y Finanzas
- ◯ Comercial
- ◯ Personas y Cultura
- ◯ Regencia y Calidad
- ◯ Visitas Médicas
- ◯ Gerencia
- ◯ Otras

2. ¿Qué tipo de sistemas de TI utiliza regularmente en sus labores diarias? (Seleccione todas las que apliquen) *

- [ ] ERP (Sistema de Planificación de Recursos Empresariales, como ser Microsoft Dynamics)
- [ ] Plataforma de correo electrónico (Outlook, Gmail)
- [ ] Herramientas de oficina (Suite de Microsoft Office)
- [ ] Otras

3. ¿Cuál de las siguientes opciones describe mejor su rol principal en la organización? *

- ◯ Liderazgo / Supervisión (tengo personal a mi cargo)
- ◯ Colaborador Técnico / Especializado (mi rol requiere conocimientos técnicos específicos)
- ◯ Colaborador Administrativo / Soporte (mi rol se centra en tareas administrativas y de soporte)

Siguiente

Página 1 de 5

Sección 2: Conocimiento y Concientizacion

4. Siguiendo una escala del 1 al 5, donde 1 representa **"Nada Importante"** y 5 representa **"Muy Importante"**, califique las siguientes afirmaciones según su criterio personal: *

	1 - **Nada Importante**	2	3	4	5 - **Muy Importante**
La ciberseguridad y la gestión de riesgos de TI contribuyen a la eficiencia operativa de la empresa.	◯	◯	◯	◯	◯
La ciberseguridad debe ser para proteger los datos de clientes y proveedores.	◯	◯	◯	◯	◯
Se debe contar con un plan de recuperación ante desastres orientados al área de TI.	◯	◯	◯	◯	◯
Se debe capacitar continuamente al personal en riesgos cibernéticos.	◯	◯	◯	◯	◯

5. Siguiendo una escala del 1 al 5, donde 1 representa **"Nada Urgente"** y 5 representa **"Muy Urgente"**, califique las siguientes situaciones según su criterio personal: *

	1 - **Nada Urgente**	2	3	4	5 - **Muy Urgente**
Un ataque de ransomware que bloquee el acceso a los sistemas de pedidos e inventario.	◯	◯	◯	◯	◯
Una filtración de datos confidenciales de clientes o productos.	◯	◯	◯	◯	◯
La caída prolongada del sistema ERP, impidiendo facturar o gestionar envíos.	◯	◯	◯	◯	◯
El error humano interno (ej.: enviar un correo importante a la persona equivocada).	◯	◯	◯	◯	◯
El incumplimiento de regulaciones farmacéuticas (ej.: trazabilidad de medicamentos).	◯	◯	◯	◯	◯

Atrás Siguiente

Página 2 de 5

Sección 3: Evaluación de Competencias

La siguiente sección tiene como propósito medir conocimientos sobre la gestión de TI a nivel técnico, por lo que si desconoce la respuesta escriba "Sin respuesta".

6. Liste 3 activos tecnológicos clave de la empresa y describa los riesgos asociados a la **confidencialidad, integridad y disponibilidad.** *

Escriba su respuesta

7. ¿Qué proceso seguiría en caso de detectar un virus dentro de los sistemas de la empresa (considere el ERP, el almacenamiento en la nube o las carpetas compartidas)? Detalle paso a paso su forma de evaluar el riesgo y las acciones que tomaría. *

Escriba su respuesta

8. En el caso hipotético de que un ex-compañero de trabajo filtre información sensible de la empresa, **proponga 3 controles** para tratar esta situación. (Tome en cuenta 3 tipos de tratamiento: **Preventivo, Detectivo y Correctivo**) *

Escriba su respuesta

Atrás Siguiente

Página 3 de 5

Sección 4: Experiencias y Practicas

9. ¿Ha recibido formación sobre cómo detectar amenazas de ciberseguridad como phishing o malware? *

- ◯ Sí, de forma regular y actualizada.
- ◯ Sí, pero hace mucho tiempo
- ◯ No, nunca.
- ◯ No estoy seguro/a.

0. En el último año, ¿ha experimentado o presenciado algún incidente relacionado con la seguridad de la información? (ej.: correo phishing, ransomware, caída de sistemas críticos, pérdida de datos) *

- ◯ Sí, en múltiples ocasiones.
- ◯ Sí, en una ocasión.
- ◯ No, nunca.
- ◯ Prefiero no responder.

Atrás | Siguiente

Página 4 de 5

Sección 5: Comentarios y Sugerencias

12. Desde su perspectiva, ¿cuál es el mayor riesgo de TI al que se enfrenta la empresa? *

Escriba su respuesta

13. ¿Qué tipo de apoyo, recursos o capacitación cree que necesita para contribuir mejor a la seguridad de la información de la empresa? *

Escriba su respuesta

Atrás | Enviar

Página 5 de 5